

**IDENTIFICACIÓN DE REQUERIMIENTOS DE TRÁFICO EN LA
PLATAFORMA TECNOLÓGICA DE LA FUNDACIÓN UNIVERSITARIA
TECNOLÓGICO COMFENALCO**

**NABY BACK MONDOL VASQUEZ
KAREN CATHERINE GUARDIOLA SEÑA**

**Monografía presentada como registro de aprobación de la
Especialización en Telecomunicaciones**

**ESPECIALIZACION EN TELECOMUNICACIONES
UNIVERSIDAD TECNOLÓGICA DE BOLIVAR
CARTAGENA DE INDIAS
2011**

**IDENTIFICACIÓN DE REQUERIMIENTOS DE TRÁFICO EN LA
PLATAFORMA TECNOLÓGICA DE LA FUNDACIÓN
UNIVERSITARIA TECNOLÓGICO COMFENALCO**

Cartagena D.T.y C. enero 18 de enero de 2011

Señores
COMITÉ DE EVALUACION DE PROYECTOS
Especialización en telecomunicaciones
UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

Cordial saludo

A través de la presente me permito la monografía titulada **IDENTIFICACIÓN DE REQUERIMIENTOS DE TRÁFICO EN LA PLATAFORMA TECNOLÓGICA DE LA FUNDACIÓN UNIVERSITARIA TECNOLÓGICO COMFENALCO** para su estudio y evaluación que fue realizada por los estudiantes **KAREN CATHERINE GUARDIOLA SEÑA** y **NABY BACK MONDOL VASQUEZ**, de la cual acepte ser su director.

Atentamente,

Eduardo Gómez Vásquez

ING. Electrónico, magister en ciencias computacionales.

Cartagena D.T.y C. enero 18 de enero de 2011

Señores

COMITÉ DE EVALUACION DE PROYECTOS
Especialización en telecomunicaciones
UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

Respetados Señores:

Presentamos para su consideración la monografía titulada: **IDENTIFICACIÓN DE REQUERIMIENTOS DE TRÁFICO EN LA PLATAFORMA TECNOLÓGICA DE LA FUNDACIÓN UNIVERSITARIA TECNOLÓGICO COMFENALCO**. Como requisito para optar el título de Especialistas en Telecomunicaciones.

Atentamente,

Naby Back Mondol Vásquez
CC. 73.181.666

Karen Catherine Guardiola Seña
CC. 45.539.883

Nota de Aceptación

Presidente del jurado

Jurado

Jurado

Agradecimientos:

Los autores expresan sus agradecimientos a:

A Dios por permitirnos cumplir con éxito todo este año de estudio en la especialización.

A la Universidad Tecnológica de Bolívar y a nuestro coordinador y director, Gonzalo López por su constante colaboración y apoyo durante el desarrollo de esta monografía.

A nuestros compañeros de la Especialización en Telecomunicaciones, por haber estado en los momentos malos y bueno durante todo este año de estudio.

A todos muchas Gracias.

TABLA DE CONTENIDO

INTRODUCCIÓN.....	9
1. OBJETIVOS.....	11
1.1 Objetivo General:.....	11
1.2 Objetivos Específicos:.....	11
2. ESTADO DEL ARTE	12
3. HERRAMIENTAS INFORMATICAS REQUERIDAS	16
3.1 Microsoft Network Monitor:	16
3.2 Wireshark	17
3.3 SNMP	18
4. DIAGRAMA ACTUAL DE LA RED.....	20
5. DESCRIPCION DE LA MUESTRA	24
6. DESCRIPCION DE TRAFICO PRESENTE EN AL RED	25
7. DIAGRAMA DE CONSUMO DE INTERNET DE LA RED ADMINISTRATIVA Y ACADEMICA.....	¡Error! Marcador no definido.43
8. ANALISIS DE TRÁFICO.....	45
8.1 Trafico de la red Académica.....	48
8.2 Clasificación del Tráfico Académico.....	51
8.3 Trafico de la red Administrativa	52
8.4 Características Equipos Activos – Conmutación	57
8.5 Consideraciones para el enlace inalámbrico	58
8.6 Servidores Recursos Elevados.....	59

CONCLUSIONES.....	61
BIBLIOGRAFÍA.....	64
LISTA DE FIGURAS	65
LISTA DE TABLAS	67

INTRODUCCIÓN

Durante el desarrollo de esta investigación se han planteado diferentes interrogantes, desde el proceso del nacimiento de la conectividad entre el cliente la red fija, hasta la integración de diferentes elementos de convergencia que integran una arquitectura cada vez más híbrida en donde el consumo del ancho de banda es mayor debido, en gran medida, a la expansión de servicios inalámbricos de uso personal como celulares, portátiles y otros dispositivos que convergen en ambientes de interoperabilidad.

Ahora bien, dentro de las aplicaciones que son utilizadas de forma más concurrente se encuentran las de aprendizaje en línea, esto debido en gran medida a la posibilidad de hacer más accesible el conocimiento y a que los usuarios cuenten con servicios de conectividad más económicos y en algunos casos gratuitos, ya que es más frecuente poder acceder a servicios conocidos como sitios públicos (hot-spot). La utilización de los modelos de aprendizaje en línea facilita el acceso a la educación de una forma más fácil, todo ello dentro de un ambiente virtual, y en algunos casos resulta ser una herramienta indispensable para muchas organizaciones. La aplicación de aprendizaje Moodle actualmente está presente en 211 países y tiene un registro de 56,819 sitios que utilizan su plataforma, según estadísticas disponibles en su portal.

Todas las aplicaciones que hoy en día se utilizan en línea generan un consumo importante del tráfico de red y provocan que el ancho de banda de las organizaciones se vea afectado de forma directa o indirecta, tanto dentro de su Intranet como los servicios de acceso a Internet; estas aplicaciones, por lo general, dependen en gran medida de la disponibilidad y continuidad de la operación de la red. Actualmente las redes de cómputo que cuentan con más de mil dispositivos en red, cuentan con técnicas que permiten optimizar sus comunicaciones, basados en el modelo jerárquico de red SONA (Service-Oriented

Network Architecture) Framework (Bruno, 2007) y el modelo PDIOO (Teare, 2005) de Cisco Systems que considera cinco elementos de diseño para arquitecturas de red como indispensables, los cuales están conformados por la fase de planeación, diseño, implementación, operación y optimización para garantizar el ciclo de vida de una red y la factibilidad de ofrecer calidad de servicio (QoS) y clase del servicio (CoS) en cada uno de los puertos físicos de la red, con el objeto de garantizar comunicaciones estables y operables. El problema que rodea al espectro inalámbrico es que actualmente el comportamiento en la zona de fresnel es muy inestable y difícil su administración en redes que utilizan el estándar IEEE 802.11 a/b/g/n para servicios Wi-Fi y el estándar IEEE 802.16 para servicios WiMax, ambos utilizando frecuencias diferentes.

1. OBJETIVOS

1.1 Objetivo General:

Identificar la capacidad de canal consumida por la sede barrio España, al igual que el tipo de tráfico que se transporta a través del backbone, con el fin de detectar el consumo real necesario y los flujos que recargan innecesariamente los equipos activos y el canal que sirve de enlace entre la sede en mención y la sede de Zaragocilla.

1.2 Objetivos Específicos:

- Tomar muestras de tráfico de los equipos activos de la red, de los servidores y de las estaciones de trabajo.
- Identificar los diferentes flujos de tráfico que son transportados a través de la red.
- Analizar el consumo de la capacidad de canal de red del tráfico identificado.
- Evaluar si la capacidad de canal que brinda la red al segmento local y hacia el backbone son suficientes para garantizar el delay, el jitter, el throughput necesario para ejecución correcta de los sistemas de información corporativos.

2. ESTADO DEL ARTE

A continuación presentamos diferentes proyectos informáticos encaminados al análisis de tráfico en redes de ordenadores.

Análisis y Caracterización de Tráfico IP en la Red Regional Ciez@netⁱ

En este trabajo, se realizó un análisis y monitorización del tráfico de Internet sobre una subred real de ciudadanos denominada Ciez@net.

El proyecto Ciez@netⁱⁱ es la primera experiencia piloto de Ciudad Digital realizada en la Región de Murcia. Ciez@net provee a sus usuarios con un acceso básico a Internet con tecnología RDSI-BE hasta el ISP (Internet Service Provider) y finalmente a través de un enlace Frame Relay. Para realizar la captura y monitorización de datos se utilizó el analizador de redes DominoWAN DA-310. Además hemos desarrollado una herramienta software para interpretar los resultadosⁱⁱⁱ.

El resultado de las medidas permitió conocer aspectos de la subred como son la carga de tráfico, direcciones web más visitadas, número de usuarios conectados, distribución de tamaño de paquetes IP, composición del tráfico por protocolo y aplicación, y distribución de la longitud de paquetes por servicios.

MIRA: Software para el análisis de tráfico IP sobre ATM^{iv}

El objetivo del proyecto MIRA es el desarrollo de una plataforma avanzada de supervisión y control de tráfico para redes académicas y de investigación. El punto de partida es el prototipo experimental MEHARI, desarrollado por los mismos grupos investigadores que participan en el proyecto MIRA. Se trata, por un lado de complementar las funcionalidades básicas del sistema MEHARI, mejorando robustez y operatividad, y por otro de ampliar sus prestaciones orientándolo a facilitar la supervisión y gestión de políticas de uso aceptable (AUP: Acceptable Use Policy) sobre redes académicas y de investigación convencionales (ej.

RedIRIS) y de nueva generación (ej. RedIRIS2 y TEN-155). En concreto, en lo concerniente a la consolidación de la plataforma existente, se está desarrollando una Interfaz Gráfica de Usuario, se están adaptando los módulos de captura para que se puedan utilizar en segmentos Ethernet y para el soporte de IPv6, se está preparando la plataforma para poder tomar medidas en varios puntos de la red para mejorar las tasas de captura actuales, etc. Referente a la ampliación de funcionalidades, el objetivo es añadir módulos de medida de consumos para tarificación, supervisión de la calidad de servicio ofrecida por la red, generación de alarmas ante determinadas situaciones y gestión de mecanismos de encaminamiento avanzados.

SMARTxAC: Sistema de monitorización y análisis de tráfico para la Anella Científica

En los últimos años, en la red académica española (RedIRIS) se han llevado a cabo diferentes proyectos relacionados con la monitorización y la caracterización del tráfico Internet, como por ejemplo los proyectos CASTBA, MEHARI y MIRA. Estos proyectos se realizaron de forma conjunta entre la Universidad Politécnica de Madrid, la Carlos III de Madrid, la Politècnica de Catalunya (UPC), y con la participación como EPOs de RedIRIS, Telefónica Investigación y Desarrollo, el Centre de Supercomputació de Catalunya (CESCA) y el Institut Català de Tecnologia.

Una vez finalizados estos proyectos y basándose en la experiencia adquirida en su participación, el Centre de Comunicacions Avanzades de Banda Amplia (CCABA) de la UPC, desarrolló un prototipo propio de un sistema completo de monitorización que permite el análisis de tráfico en tiempo real en enlaces de alta velocidad. Este prototipo proporciona información detallada sobre el uso que se hace de la red monitorizada, información que puede ser de gran ayuda para el dimensionado y la optimización de recursos, además de ser útil para detectar usos irregulares y ataques.

El funcionamiento de este prototipo se probó en el troncal de Cataluña de RedIRIS (Anella Científica), que constituye la principal vía de salida a Internet de las universidades y centros de investigación catalanes. Los resultados de estas primeras pruebas fueron muy satisfactorios y animaron a los gestores de la Anella Científica (CESCA) a encargar al CCABA-UPC el desarrollo de una versión mejorada de dicho sistema, que ha dado lugar al proyecto SMARTxAC.

El proyecto SMARTxAC es un acuerdo de colaboración entre el CESCA y la UPC, que se inició en julio de 2003, con el objetivo de instalar una versión del prototipo desarrollado en el CCABA-UPC para la monitorización permanente de la Anella Científica. Este nuevo sistema deberá proporcionar información útil que ayude al CESCA en las tareas diarias de gestión de la red.

La funcionalidad principal del sistema SMARTxAC es la monitorización y el análisis de tráfico en tiempo real en enlaces troncales de alta velocidad. Estos enlaces son compartidos por gran cantidad de redes, que a su vez están dando servicio a miles de usuarios. Estos usuarios tienen necesidades y perfiles muy diferentes, y pueden acceder a una gran variedad de servicios. Debido a esta heterogeneidad, no sólo el volumen de tráfico presente en estas redes es muy elevado, sino que también lo es el número de sesiones establecidas simultáneamente. Precisamente, la gran cantidad y variedad de datos a capturar y analizar es la principal dificultad a abordar en el desarrollo de un sistema de estas características. El equipo de captura debe ser capaz de capturar todo el tráfico, sin perder ningún paquete, pero la dificultad principal está en el sistema de análisis, que debe ser lo suficientemente ligero y eficiente para poder tratar toda esta información en tiempo real, y resumirla para que sea viable su almacenamiento de forma permanente.

Llamamos plataforma de captura a la parte hardware y software dedicado a la captura de tráfico. Al igual que en el proyecto MIRA, se realiza una captura pasiva (no intrusiva) del tráfico, utilizando divisores de fibra pasivos (splitters), que permiten enviar una copia íntegra del tráfico a un PC, que se encarga de la

captura y el procesado de los paquetes. Al contrario de lo que sucede con otras técnicas de captura, como Cisco NetFlow o los basados en SNMP, nuestro sistema no afecta en absoluto al rendimiento de la red monitorizada, ya que la captura no se realiza directamente en los equipos dedicados a la interconexión de redes, ni tampoco se genera tráfico adicional.

Se ha desestimado utilizar la plataforma de captura desarrollada en el proyecto MIRA, debido a que los requisitos actuales difieren de forma considerable con los que se plantearon en dicho proyecto. El sistema MIRA realizaba una captura estadística del tráfico (aproximadamente un 10% del tráfico real) debido a que se capturaba el contenido de los paquetes. En el sistema SMARTxAC se ha preferido capturar únicamente las cabeceras de los paquetes, y conseguir así una captura completa del tráfico, utilizando el software de libre distribución CoralReef. De esta forma, las cabeceras capturadas pueden agregarse en forma de flujos, y reducir así el volumen de datos a tratar por el sistema de análisis. Pero además, la captura de contenidos también presenta varias limitaciones, como la posible infracción de confidencialidad o la imposibilidad de analizar los paquetes cifrados mediante técnicas de encriptación.

-
- i. María Dolores Cano, Josemaría Malgosa Sanahuja, Fernando Cerdán, Joan García Haro
Universidad Politécnica de Cartagena. Departamento de Tecnologías de la Información y las Comunicaciones. Campus
Muralla del Mar s/n (Ed. Hospital de Marina) 30202 Cartagena, España
“The Ciez@net project”. <www.f-integra.org/projects.htm#ciezanet>
- ii. Josemaría Malgosa-Sanahuja, María-Dolores Cano, Fernando Cerdán, Joan García-Haro. “TAT, Traffic
Analysis Tool For the Statistics Analysis of IP Networks”. Proceedings of IEEE PACRIM '01
- iii. Carles Veciana, Josep Solé Pareta, Sergi Sales, Jordi Domingo. Universitat Politècnica de Catalunya (UPC),
iv. Jordi Girona 1-3, 08034 Barcelona. {carlosv,pareta,ssales,jordid}@ac.upc.es, Arturo Azcorra, Alberto García.
Universidad Carlos III de Madrid (UC3M), Butarque 15, 28911 Leganés (Madrid).
{azcorra,alberto}@it.uc3m.es. Telefónica Investigación y Desarrollo. paag@tid.es

3. HERRAMIENTAS INFORMATICAS REQUERIDAS

El uso de herramientas para análisis de tráfico, se justifica dada la situación de que en la red se encontraban las siguientes anomalías:

- Colisiones
- Perdida de paquetes
- Servicios no identificados
- Inestabilidad de la red y servicios principales

Por tal motivo se hace necesario el uso de las siguientes herramientas que nos darán una noción clara de lo que se quiere con este Trabajo integrador.

3.1 Microsoft Network Monitor:

Microsoft Network Monitor es un Aplicación que te permitirá visualizar y analizar los protocolos de Comunicación que se presentan entre los diferentes equipos que conforman una red de datos. Es decir, podrás visualizar los diálogos que cada uno de los protocolos requiere para establecer la comunicación o atender a una petición determinada. Es un analizador de protocolos de tráfico web, con el cual podemos medir los tiempos de envío y recepción de paquetes y de los procesos relacionados a la red (es decir, todos aquellos que están generando movimiento de datos, o flujo de información).

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=983b941d-06cb-4658-b7f6-3088333d062f>

3.2 Wireshark

Es un completo analizador de red y de tráfico, surgido en Linux bajo el nombre de Ethernet pero que con el tiempo y junto con su cambio al nombre actual ha pasado a ser multiplataforma. Wireshark 1.2 es open source, y hay versiones para Linux, Mac OS X y Windows.

<http://www.wireshark.org/>

Figura N° 1 Microsoft Network Monitor

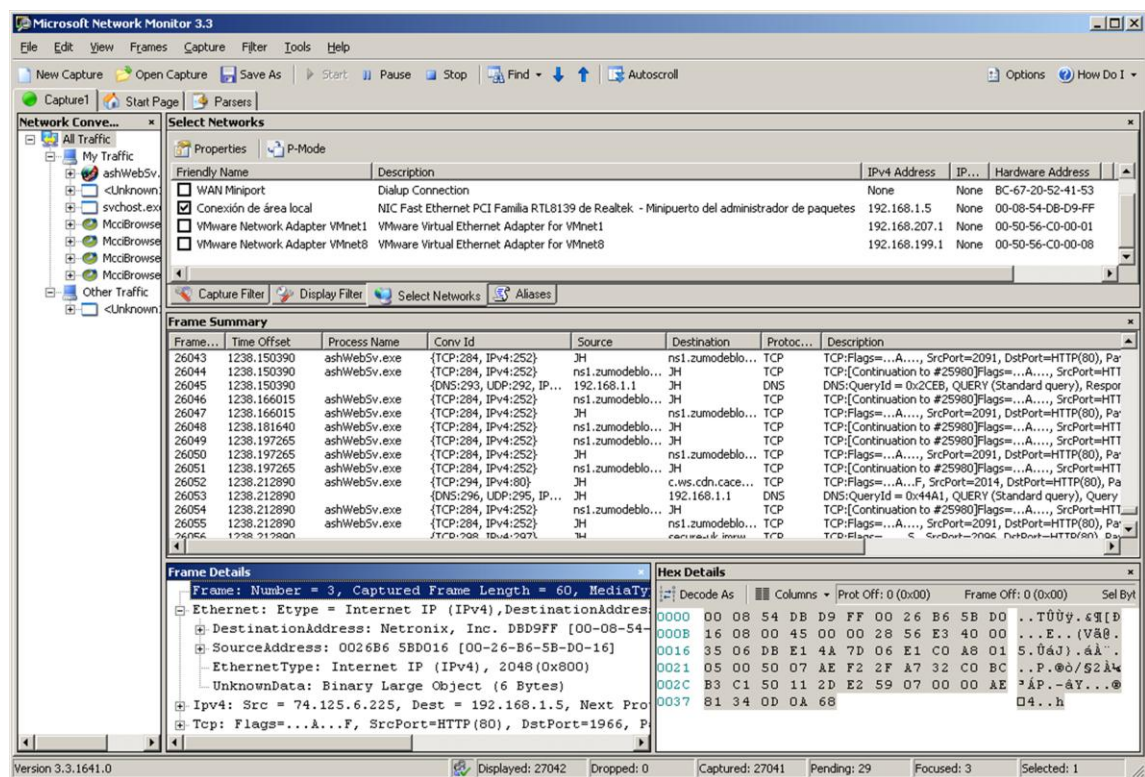
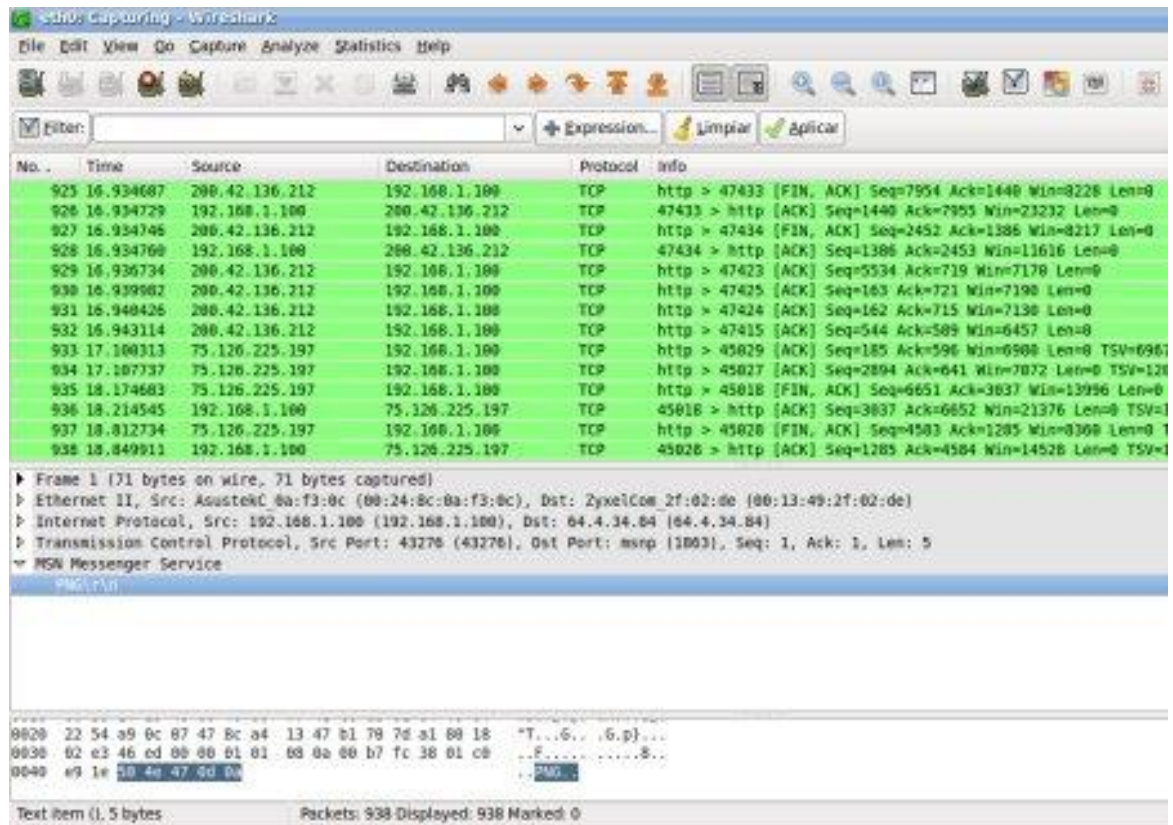


Figura N° 2 Captura de Trafico



Wireshark - <http://www.wireshark.org/>

3.3 Agente SNMP

SNMP (Simple Network Management Protocol) es un protocolo ampliamente utilizado en la administración de redes para supervisar la salud y el bienestar del equipo de la red, equipo de cómputo y otros dispositivos.

Una red administrada a través de SNMP consiste de tres componentes claves:

Dispositivos administrados;

Agentes;

Sistemas administradores de red (NMS's).

Figura N° 3 Snmp (Manager <==> Agente)

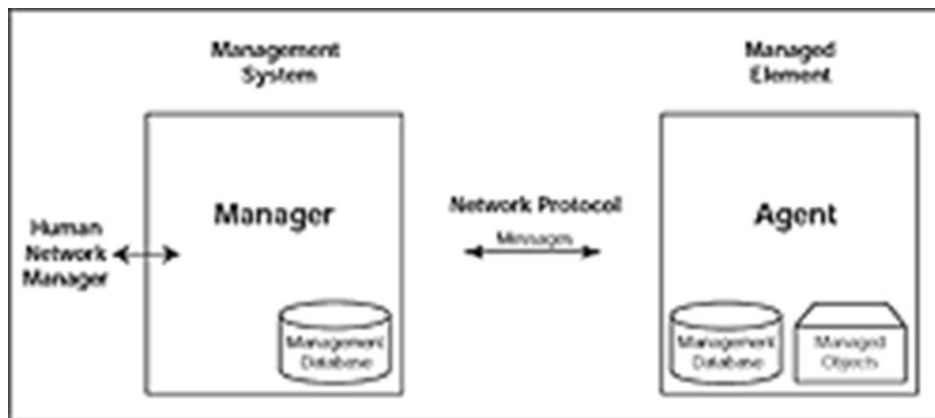


Ilustración 1

Un dispositivo administrado es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

Un NMS ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada.

4. DIAGRAMA ACTUAL DE LA RED

Capacidad Tecnológica

El sistemas de comunicación (LAN) de la Fundación Universitaria Tecnológico Comfenalco se interconecta básicamente por cable UTP categoría 6A, Fibra Óptica, Switches capa (3), Routers, Firewall, servidores y Antenas de Radio enlace; su infraestructura está apoyada en una red conmutada en topología Jerárquica. La red de voz esta soportada por cable UTP categoría 6 y es administrada por una central telefónica PBX digital-análoga marca Panasonic la cual está conectada por un equipo de cómputo donde se gestiona y se configura las extensiones, grupo, tiempo etc.

Topología de la red de comunicación

La arquitectura de la red informática y el medio de comunicación interna que utiliza el Tecnológico Comfenalco está basado en cable UTP categoría 6, 6A y la normativa que se maneja es la T568B, con velocidades de 10 Mbps - 100 Mbps – 1000 Mbps, la topología de red implementada es la topología Árbol, además se cuenta con un Backbone que va desde el Data Center hasta un piso superior del edificio. La red LAN del Tecnológico se encuentra dividida en dos subredes, Área Administrativa y la Académica, esto se hace mediante un Switch Core Cat4500 E-Series 7-Slot Chassis de capa 3 y 4 De 48 y 24 puertos.

Acceso a Internet

El servicio de Internet es suministrado por Telefónica Telecom con un canal dedicado 1:1 de 4 Mbps y Columbus con un canal de 10 Mbps. Para proporcionar el servicio de Internet a la sede de Zaragocilla se utiliza un Radio Enlace, las señales son enviadas a través de antenas ubicadas en zonas altas tanto de la sede principal (sede España) como en la sede Zaragocilla para lograr una buena línea de vista, esta es aterrizada por un cable UTP categoría 5A que se interconecta a un Switch 3Com 4500G capa 3 de 24 puertos, este tiene configurado Vlans para segmentar la información tanto para el área administrativa como para el área de estudiantes.

Computadores

En cada departamento o sección se dispone de un computador por usuario, generalmente son computadores de escritorio, sin embargo, existe un gran número de usuarios como gerentes, asistentes, Jefe, Directores entre otros, que necesitan movilizarse dentro de la Institución e incluso a la sede de zaragocilla, por esta razón este tipo de usuarios disponen de computadores portátiles.

En el área Administrativa se cuenta con 145 Computadores de mesa y 50 portátil para un total de 195 equipos de cómputos. El área Académica cuenta con 342 computadores y 50 portátil para un total de 392 equipos de cómputos.

Servidores

Los servidores se encuentran ubicados en el cuarto de comunicaciones de la Fundación Universitaria Tecnológico Comfenalco, estos presta servicios como: Web tecnológico Comfenalco, Plataforma virtual, Conexiones Cartagena, Exchange Server, Portal Institucional (SharePoint), Dhcp Académico, Dhcp Administrativo, Servido de Almacenamiento, Syneris, Proxy académico, Proxy Administrativo, DNS, Antivirus, ERP, Nomina entre otros.

Sistemas Operativos en Servidores

En los servidores que se tiene están instalados los siguiente sistemas operativo, Linux Centos 5,1, Windows 2003 Server R2, Windows 2008 Server, Linux Red hat 9, donde se administra y se gestiona todo los recursos y servicios que la institución ofrece.

Marcas de los Servidores

Los servidores con los que cuenta la red del Tecnológico Comfenalco son de diferentes marcas entre los que encontramos:

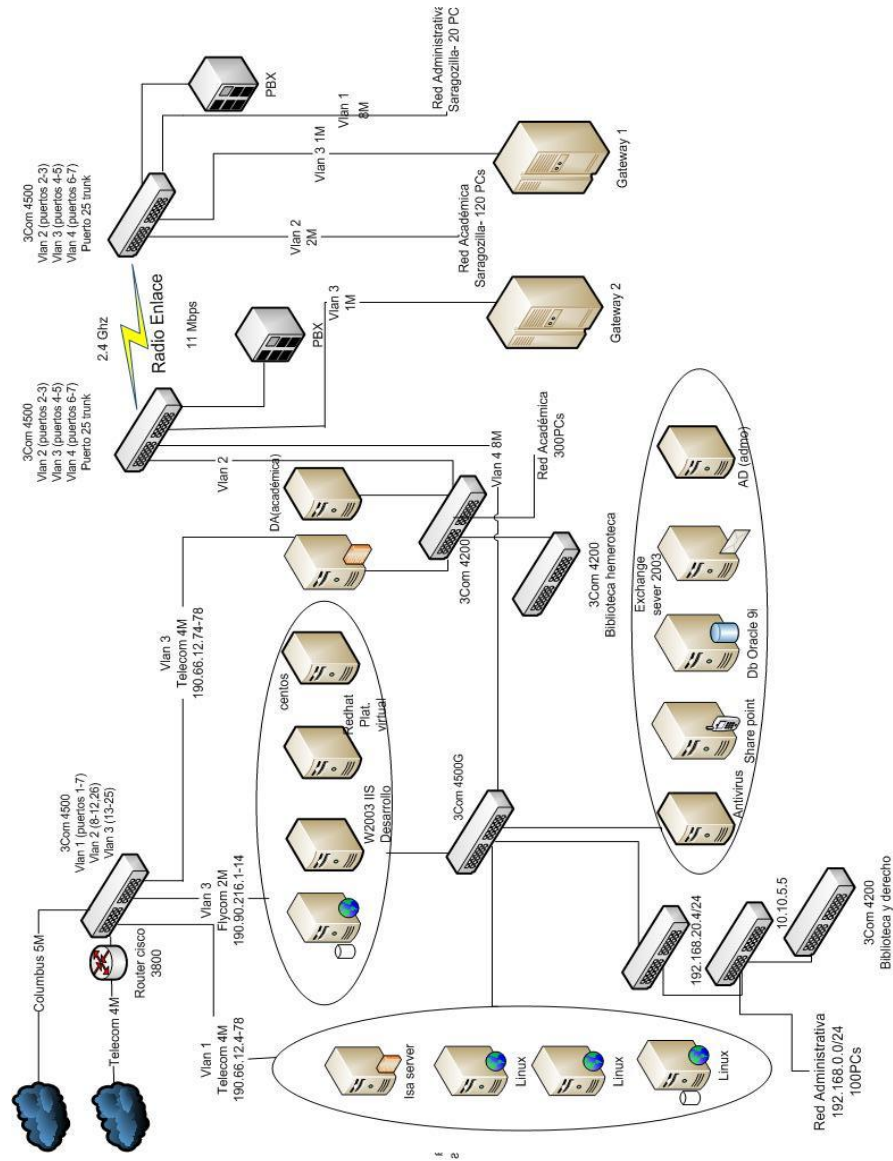
- 2 HP Blade System C3000 Enclousure, con 11 servidores
- HP Storage works P2000
- DELL: se cuenta con los siguientes modelos (PowerEdge R200, PowerEdge 2950, PowerVault MD1000, Proliant ML350 G4, PowerEdge 1600SC, PowerEdge 600SC, entre otros).

Servicios que se Ejecutan y Aplicaciones

Los servicios que se tiene configurado en los diferentes servidores ya mencionado tenemos:

- ✓ Apache 2.0/Tomcat 5.5.25/PHP 4.3.9/Java 1.5.0_14/Mysql 4.1.20
Aplicaciones:
 - Web Conexiones Cartagena / Saepro / Sedoc / Swap / Moodle
- ✓ Exchange 2003 Server/PDC y DNS Primario
Aplicaciones:
 - Exchange Server 2007
- ✓ ISA server
Aplicaciones:
 - Isa server 2006 Firewall
- ✓ SharePoint /Consola Antivirus
- ✓ Controlador De Dominio/DHCP/DNS/
- ✓ Copias Syneris/ Dependencias Backup Exchange
- ✓ Oracle 9i
- ✓ DHCP /Dominio y DNS Secundario
- ✓ Samba Server

Figura N° 4 Diagrama de Red



Microsoft Visio Software 2007

5. DESCRIPCION DE LA MUESTRA

Se consideró pertinente por el tamaño de la red y el tiempo del servicio la toma de una muestra significativa de alrededor del 60% de las estaciones pertenecientes a la red administrativa y a la red académica de las sedes del barrio España y Zaragocilla de la institución.

Por otro lado se tomó la totalidad de los servidores y el core de los equipos activos de la red ubicados en el barrio España para la toma de tráfico debido a su vital importancia en el buen funcionamiento de la red a través de herramientas propietarias y de la habilitación de algunos servicios del sistema operativo logramos recolectar la información necesaria para la elaboración del presente trabajo.

6. DESCRIPCION DE TRAFICO PRESENTE EN AL RED

A continuación se relacionan y se explican de forma breve todos los tipos de tráfico encontrados en la inspección realizada a la red de la institución tecnológico Comfenalco al momento de este estudio:

0x88a7 (cluster)

Figura N° 5 Trafico 0x88a7

398 136.622187	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_0a	0x88a7	Ethernet II
563 196.619663	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_0a	0x88a7	Ethernet II
742 256.616920	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_0a	0x88a7	Ethernet II
905 316.863668	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_0a	0x88a7	Ethernet II
1082 376.861137	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_0a	0x88a7	Ethernet II
1241 436.859071	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_0a	0x88a7	Ethernet II
1422 496.916458	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_0a	0x88a7	Ethernet II

Se están generando tramas Ethernet con el campo type=0x88a7 en switch 3com donde se tiene configurado Vlan de la compañía, este valor debería cambiarse al equivalente a 802.1q el cual es 0x8100 para evitar recibo y forwarding de paquete de manera caótica, este cambio se debe realizar ajustando la configuración de las vlan en este dispositivo.

Dirección(es) origen: 3com:c9:0e:8b, 3comeuro:c9:0e:8c

Dirección(es) destino: 01:80:c2:00:00:0a

ARP

Figura N° 6 Trafico ARP

40 12.445969	QuantaCo_1e:5a:a3	Broadcast	ARP	Who has 192.168.0.73? Tell 192.168.0.74?
41 12.548417	Dell_92:e1:fd	Broadcast	ARP	Who has 192.168.0.74? Tell 192.168.0.74?
42 13.201315	Dell_d3:5e:b5	Broadcast	ARP	Who has 192.168.0.202? Tell 192.168.0.74?
43 13.546665	Dell_92:e1:fd	Broadcast	ARP	Who has 192.168.0.74? Tell 192.168.0.74?
45 14.841435	Dell_92:e1:fd	Broadcast	ARP	Who has 192.168.0.74? Tell 192.168.0.74?
46 14.947293	Dell_83:56:66	Broadcast	ARP	Who has 192.168.0.129? Tell 192.168.0.129?
54 15.485449	Dell_83:56:66	Broadcast	ARP	Who has 192.168.0.129? Tell 192.168.0.129?
55 15.558794	Dell_92:e1:fd	Broadcast	ARP	Who has 192.168.0.74? Tell 192.168.0.74?

Address Resolution Protocol-Protocolo de resolución de direcciones: Es un protocolo de nivel 3 responsable de encontrar la dirección hardware que corresponde a una determinada IP. Para ello se envía una trama (ARP request) a la dirección de multidifusión de la red (broadcast (MAC = ff ff ff ff ff)) conteniendo la IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección MAC que le corresponde.

Cada máquina mantiene una cache con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección IP ser independiente de la dirección MAC, pero esto solo funciona si todas las máquinas lo soportan.

dirección(es) origen: varias

dirección(es) destino: ff:ff:ff:ff:ff:ff

Se están generando ARP Gratuitos desde los switch 3COM con las siguientes MAC

00:1e:c1:c9:a7:41

00:1e:c1:c9:0e:81

BROWSER

Figura N° 7 Trafico BROWSER

581 201.517653	192.168.0.139	192.168.0.255	BROWSER	Host Announcement ESPRE01, Worl
757 259.629202	192.168.0.66	192.168.0.255	BROWSER	Host Announcement MAGDALENA, W
1124 388.922859	192.168.0.109	192.168.0.255	BROWSER	Host Announcement ESBIB04, Worl
1211 426.814981	192.168.0.28	192.168.0.255	BROWSER	Host Announcement ESCAR06, Worl
1353 476.814100	192.168.0.41	192.168.0.255	BROWSER	Host Announcement ESTEC01, Worl
1379 485.013434	192.168.0.60	192.168.0.255	BROWSER	Host Announcement CTGSP01, Worl
1394 489.516589	192.168.0.110	192.168.0.255	BROWSER	Host Announcement ESBIB08, Worl
1395 489.569313	192.168.0.205	192.168.0.255	BROWSER	Host Announcement ARIARI, Work
1512 528.915644	192.168.0.121	192.168.0.255	BROWSER	Domain/Workgroup Announcement t

Microsoft Windows Browser Protocol- Protocolo de búsqueda de Microsoft Windows: Protocolo de capa de aplicación que funciona en capa de transporte sobre UDP y utiliza el puerto 138 para el intercambio de mensajes. La función principal del servicio es proporcionar una lista de equipos que comparten recursos en el dominio de un cliente junto con una lista de otros nombres de dominio y de

grupo de trabajo de la red de área extensa (WAN). Esta lista se proporciona a los clientes que ven recursos de red con Entorno de red o con el comando NET VIEW.

Dirección(es) origen: varias

Dirección(es) destino: ff:ff:ff:ff:ff:ff

CDP

Figura N° 8 Trafico CDP - Cisco Discovery Protocol

621 213.523798	Cisco_e1:e7:cf	CDP/VTP/DTP/PagP/UDLD	CDP	Device ID: esser01	Port ID: Fa
798 273.522377	Cisco_e1:e7:cf	CDP/VTP/DTP/PagP/UDLD	CDP	Device ID: esser01	Port ID: Fa
962 333.519278	Cisco_e1:e7:cf	CDP/VTP/DTP/PagP/UDLD	CDP	Device ID: esser01	Port ID: Fa
1132 393.521842	Cisco_e1:e7:cf	CDP/VTP/DTP/PagP/UDLD	CDP	Device ID: esser01	Port ID: Fa
1288 453.538248	Cisco_e1:e7:cf	CDP/VTP/DTP/PagP/UDLD	CDP	Device ID: esser01	Port ID: Fa
1468 513.548136	Cisco_e1:e7:cf	CDP/VTP/DTP/PagP/UDLD	CDP	Device ID: esser01	Port ID: Fa
1675 573.587405	Cisco_e1:e7:cf	CDP/VTP/DTP/PagP/UDLD	CDP	Device ID: esser01	Port ID: Fa
1897 633.584109	Cisco_e1:e7:cf	CDP/VTP/DTP/PagP/UDLD	CDP	Device ID: esser01	Port ID: Fa
2080 693.618773	Cisco_e1:e7:cf	CDP/VTP/DTP/PagP/UDLD	CDP	Device ID: esser01	Port ID: Fa

Cisco Discovery Protocol, ‘protocolo de descubrimiento de Cisco’: es un protocolo propietario de nivel 2, desarrollado por Cisco y usado en la mayoría de sus equipos. Es utilizado para compartir información sobre otros equipos Cisco directamente conectados, tal como la versión del sistema operativo y la dirección de red IP. CDP también puede ser usado para realizar (ODR, *On-Demand Routing*), que es un método para incluir información de encaminamiento en anuncios CDP, de forma que los protocolos de ruteo dinámico no necesiten ser usados en redes simples.

Los dispositivos Cisco envían anuncios a la dirección de destino multicast 01:00:0C:CC:CC:CC (que también es usada por otros protocolos propietarios de Cisco tales como VTP). Los anuncios CDP (si está soportado y configurado) se envían por defecto cada 60 segundos en las interfaces que soportan cabeceras SNAP, incluyendo Ethernet, Frame Relay y ATM. Cada dispositivo Cisco que soporta CDP almacena la información recibida de otros dispositivos en una tabla.

La información de la tabla CDP se refresca cada vez que se recibe un anuncio y la información de un dispositivo se descarta tras tres anuncios no recibidos por su parte (tras 180 segundos usando el intervalo de anuncio por defecto).

(SSDP) Simple service discovery protocol es un protocolo UPnP, utilizado en Windows XP y diferentes marcas de equipos de red. A pesar del nombre, se le considera complejo y requiere mayor esfuerzo para implementarse que DNS-SD. SSDP utiliza notificaciones HTTP que entregan una URI de tipo de servicio y un

nombre de servicio único (Unique Service Name, USN). Apoya las funciones del protocolo apipa.

dirección(es) origen: cisco:e1:e7:cf
dirección(es) destino: 01:00:0c:cc:cc:cc

CLDAP

Figura N° 9 Trafico CLDAP (Lightweight Directory Access Protocol)

66233	548.878333	192.168.0.65	192.168.0.13	CLDAP	searchResEntry(92) *<R00T>* se
66266	549.019268	192.168.0.13	192.168.0.65	CLDAP	searchRequest(93) *<R00T>* bas
66267	549.019929	192.168.0.65	192.168.0.13	CLDAP	searchResEntry(93) *<R00T>* se
102703	849.474773	192.168.0.13	192.168.0.65	CLDAP	searchRequest(94) *<R00T>* bas
102704	849.475579	192.168.0.65	192.168.0.13	CLDAP	searchResEntry(94) *<R00T>* se
139657	1150.053122	192.168.0.13	192.168.0.65	CLDAP	searchRequest(95) *<R00T>* bas
139658	1150.054094	192.168.0.65	192.168.0.13	CLDAP	searchResEntry(95) *<R00T>* se
235069	2104.626676	192.168.0.13	192.168.0.65	CLDAP	searchRequest(96) *<R00T>* bas
235072	2104.627745	192.168.0.65	192.168.0.13	CLDAP	searchResEntry(96) *<R00T>* se

Lightweight Directory Access Protocol- Protocolo de acceso a directorio ligero: El protocolo CLDAP fue diseñado para complementar la versión 2 de LDAPv2, esta dirigido a aplicaciones que requieren una búsqueda de pequeñas cantidades de información existente en el directorio.

dirección(es) origen: 00:13:d4:34:c9:48
dirección(es) destino: 00:c0:9f:1e:5a:a3

DCERPC

Figura N° 10 Trafico DCERPC

50263	413.561731	192.168.0.66	192.168.0.13	DCERPC	Response: call_id: 189 ctx_id:
50306	414.562575	192.168.0.13	192.168.0.66	DCERPC	Request: call_id: 191 opnum: 0
65888	547.241523	192.168.0.13	192.168.0.65	DCERPC	Bind: call_id: 1 EPMv4 V3.0
65889	547.242211	192.168.0.65	192.168.0.13	DCERPC	Bind ack: call_id: 1 accept ma
65903	547.295816	192.168.0.13	192.168.0.65	DCERPC	Bind: call_id: 1 DR5UAPI V4.0
65906	547.297752	192.168.0.65	192.168.0.13	DCERPC	Bind_ack: call_id: 1 accept ma
65907	547.297969	192.168.0.13	192.168.0.65	DCERPC	Alter context: call_id: 1 DR5U

DCERPC es un mecanismo estándar del IPC para las redes de Windows. Es utilizado para la autenticación, Microsoft Exchange, impresión entre otros.

dirección(es) origen:00:19:b9:f9:b8:70
dirección(es) destino: 00:13:d4:34:c9:48

DRSUAPI

Figura N° 11 Trafico DRSUAPI

302283	6968.842085	10.10.0.125	10.10.0.11	DRSUAPI	DsBind request
302284	6968.842510	10.10.0.11	10.10.0.125	DRSUAPI	DsBind response
302285	6968.842674	10.10.0.125	10.10.0.11	DRSUAPI	DsCrackNames request
302286	6968.843251	10.10.0.11	10.10.0.125	DRSUAPI	DsCrackNames response
302287	6968.843355	10.10.0.125	10.10.0.11	DRSUAPI	DsCrackNames request
302288	6968.843863	10.10.0.11	10.10.0.125	DRSUAPI	DsCrackNames response
302289	6968.843958	10.10.0.125	10.10.0.11	DRSUAPI	DsUnbind request
302290	6968.844222	10.10.0.11	10.10.0.125	DRSUAPI	DsUnbind response

Protocolo de capa de aplicación que trabaja sobre TCP y utiliza los puertos 1420,1026 para el intercambio de mensajes entre domains controllers.

dirección(es) origen:00:23:ae:92:5b:dd, 00:13:d4:34:ce:52, 00:13:d4:34:c9:48
dirección(es) destino: 00:19:b9:db:da:d5

DHCP

Figura N° 12 Trafico DHCP (Dinamic Host Configuration Protocol)

496	174.634056	192.168.0.109	255.255.255.255	DHCP	DHCP Inform - Transaction ID
667	232.108217	192.168.0.194	255.255.255.255	DHCP	DHCP Inform - Transaction ID
672	235.104614	192.168.0.194	255.255.255.255	DHCP	DHCP Inform - Transaction ID
967	337.963813	192.168.0.247	255.255.255.255	DHCP	DHCP Inform - Transaction ID
1594	546.006073	192.168.0.194	255.255.255.255	DHCP	DHCP Inform - Transaction ID
1613	551.002300	192.168.0.194	255.255.255.255	DHCP	DHCP Inform - Transaction ID
1907	638.410231	192.168.0.247	255.255.255.255	DHCP	DHCP Inform - Transaction ID

Dinamic Host Configuration Protocol-Protocolo de Configuración Dinamica de Host version 4: Protocolo que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo Cliente / Servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuanto tiempo la ha tenido, a quien se la ha asignado después.

dirección(es) origen: varias
dirección(es) destino: ff:ff:ff:ff:ff

DHCPv6

Figura N° 13 DHCP Ver 6 (Dynamic Host Configuration Protocol v6)

560 195.782787	fe80::1c9b:65a2:a434: ff02::1:2	DHCPv6	Solicit
564 197.794965	fe80::1c9b:65a2:a434: ff02::1:2	DHCPv6	Solicit
582 201.803766	fe80::1c9b:65a2:a434: ff02::1:2	DHCPv6	Solicit
610 209.807451	fe80::1c9b:65a2:a434: ff02::1:2	DHCPv6	Solicit
660 225.811160	fe80::1c9b:65a2:a434: ff02::1:2	DHCPv6	Solicit
697 240.874709	fe80::221:5aff:fe8f:e ff02::1:2	DHCPv6	Solicit
744 257.818511	fe80::1c9b:65a2:a434: ff02::1:2	DHCPv6	Solicit
889 313.352653	fe80::f493:483b:bfa0: ff02::1:2	DHCPv6	Solicit
891 314.342038	fe80::f493:483b:bfa0: ff02::1:2	DHCPv6	Solicit

Dinamic Host Configuration Protocol v6-Protocolo de Configuración Dinamica de Host version 6: Tiene la misma función que su antecesor pero funciona para el protocolo de internet vesion 6, Ipv6.

Dirección(es) origen: 00:21:5a:8f:e9:ea, 00:21:70:92:e1:fd, 00:13:21:1b:db:a9
dirección (es) destino: 33:33:00:01:00:02

DNS

Figura N° 14 Trafico DNS (Domain Name Service)

2291 755.240013	192.168.0.64	192.168.0.45	DNS	Standard query response, No su
2296 755.566545	192.168.0.45	192.168.0.64	DNS	Standard query A 0.220f6001.c0
2297 755.706952	192.168.0.64	192.168.0.45	DNS	Standard query response, No su
2298 756.125471	192.168.0.45	192.168.0.64	DNS	Standard query A 0.22097001.c0
2299 756.362556	192.168.0.64	192.168.0.45	DNS	Standard query response A 127.
2302 757.416682	192.168.0.45	192.168.0.64	DNS	Standard query A 0.220f7001.90
2303 757.540280	192.168.0.64	192.168.0.45	DNS	Standard query response A 127.
2307 759.824121	192.168.0.45	192.168.0.64	DNS	Standard query A 0.22091001.c0

Domain Name Service-Servicio de Resolucion de nombres: Protocolo de capa de aplicación que provee el servicio de resolución de nombres totalmente qualificados a direcciones IPv4 y viceversa.

Dirección(es) origen: varias
dirección(es) destino: 00:13:72:61:77:42

EPM

Figura N° 151 Trafico EPM (EndPoint Mapper- Mapeador de punto final)

262141 5884.091280	10.10.0.125	10.10.0.11	EPM	Map request
262142 5884.091627	10.10.0.11	10.10.0.125	EPM	Map response
302272 6968.838696	10.10.0.125	10.10.0.11	EPM	Map request
302273 6968.839022	10.10.0.11	10.10.0.125	EPM	Map response
302291 6968.845340	10.10.0.125	10.10.0.11	EPM	Map request
302292 6968.845674	10.10.0.11	10.10.0.125	EPM	Map response
317251 7463.793395	10.10.0.125	10.10.0.11	EPM	Map request

EndPoint Mapper- Mapeador de punto final:EPM o Epmmap es un protocolo de capa de aplicación que utiliza en capa de transporte el protocolo TCP y el puerto 135 para la llamada a procedimientos remotos RPC, este protocolo es utilizado por AD(Active Directory) para descubrir conexiones activas.

Dirección(es) origen: 00:23:ae:92:5b:dd, 00:13:d4:34:c9:48

Dirección(es) destino: 00:19:b9:db:da:d5

HTTP

Figura N° 16 Trafico HTTP (Hypertext Transfer Protocol)

579 13.226315	10.10.0.2	10.10.0.200	HTTP	HTTP/1.0 200 Connection establ
580 13.226356	10.10.0.2	10.10.0.200	HTTP	HTTP/1.0 200 Connection establ
627 14.282547	10.10.0.2	10.10.0.147	HTTP	Continuation or non-HTTP traff
633 14.386270	10.10.0.2	10.10.0.147	HTTP	Continuation or non-HTTP traff
634 14.386394	10.10.0.2	10.10.0.147	HTTP	Continuation or non-HTTP traff
1426 33.112993	10.10.0.2	10.10.1.63	HTTP	Continuation or non-HTTP traff
2326 53.330454	10.10.0.2	10.10.1.63	HTTP	Continuation or non-HTTP traff

Hypertext Transfer Protocol-Protocolo de transferencia de Texto: Este protocolo hace parte de la capa de aplicación y utiliza comúnmente el puerto 80 TCP, pero para este caso este tráfico demuestra la utilización de un servicio de proxy que utiliza el puerto 8080, este servicio tiene como objetivo permitir trafico web para los clientes

Dirección(es) origen: 3com:b5:f0:40, 00:13:d4:34:c9:48, 00:19:b9:db:da:9b

Dirección(es) destino: varias

ICAP

Figura N° 17 Trafico ICAP (Internet Content Adaptation Protocol)

2549 58.239388	10.10.0.11	10.10.0.196	ICAP	Continuation
88431 1923.122650	10.10.0.2	10.10.0.223	ICAP	Continuation
88432 1923.122774	10.10.0.2	10.10.0.223	ICAP	Continuation
88433 1923.122872	10.10.0.2	10.10.0.223	ICAP	Continuation
144061 2938.259664	10.10.0.11	10.10.0.196	ICAP	[TCP Previous segment lost] c
152120 3058.259790	10.10.0.11	10.10.0.196	ICAP	[TCP Previous segment lost] c
189946 3718.260653	10.10.0.11	10.10.0.196	ICAP	[TCP Previous segment lost] c
264041 5938.263782	10.10.0.11	10.10.0.196	ICAP	[TCP Previous segment lost] c

Internet Content Adaptation Protocol- Protocolo de adaptacion de contenidos de Internet: Este es un protocolo de capa de aplicación sobre TCP que utiliza el puerto 1344 para su funcionamiento. Este permite la redirección de contenidos con fines de filtrado y conversión, su uso generalmente es para soluciones de antivirus, filtrado de contenidos, traducción dinámica de páginas, inserción automática de anuncios, compresión de HTML, etc.

Dirección(es) origen:00:19:b9:db:da:d5, 3com:b5:f0:40

Dirección(es) destino: 00:23:ae:75:36:b9, 00:19:d1:06:a9:77

ICMP

Figura N° 18 Trafico (Internet Control Message Protocol)

263104 5910.622575	10.10.0.125	10.10.0.11	ICMP	Destination unreachable (Port
263632 5926.623171	10.10.0.125	10.10.0.11	ICMP	Destination unreachable (Port
264234 5944.622469	10.10.0.125	10.10.0.11	ICMP	Destination unreachable (Port
264965 5970.866965	10.10.0.11	10.10.0.125	ICMP	Destination unreachable (Port
265021 5972.366915	10.10.0.11	10.10.0.125	ICMP	Destination unreachable (Port
265073 5973.866873	10.10.0.11	10.10.0.125	ICMP	Destination unreachable (Port

Internet Control Message Protocol- Protocolo de control de mensajes de Internet: Protocolo de capa de red que sirve para probar funcionalidad desde capa fisica hasta capa de red para Ipv4 de un host a otro mediante un sistema de pregunta(ICMP Request) y respuesta(ICMP Reply).

Dirección(es) origen: 00:19:b9:db:da:d5, 00:19:d1:06:a2:a3,00:1a:a0:0a:91:34, 00:1a:a0:10:73:db, 00:13:d3:92:ee:c9, 00:21:97:4a:83:63, 00:21:97:62:59:8b

dirección(es) destino: 00:23:ae:92:5b:dd, 00:23:ae:92:5b:dd

ICMPv6

Figura N° 19 Trafico (Internet Control Message Protocol)

88	1.422910	fe80::71bc:d991:f124:ff02::1:ffbf:729b	ICMPv6	Neighbor solicitation
293	6.291672	fe80::71bc:d991:f124:ff02::1:ffbf:729b	ICMPv6	Neighbor solicitation
322	6.929453	fe80::71bc:d991:f124:ff02::1:ffbf:729b	ICMPv6	Neighbor solicitation
360	7.928006	fe80::71bc:d991:f124:ff02::1:ffbf:729b	ICMPv6	Neighbor solicitation
859	20.196189	fe80::1843:980f:1eb:7ff02::1:ffbf:729b	ICMPv6	Neighbor solicitation
900	20.979447	fe80::1843:980f:1eb:7ff02::1:ffbf:729b	ICMPv6	Neighbor solicitation
956	21.971957	fe80::1843:980f:1eb:7ff02::1:ffbf:729b	ICMPv6	Neighbor solicitation

Internet Control Message Protocol- Protocolo de control de mensajes: Este protocolo tiene básicamente la misma funcionalidad que ICMPv4 pero para la nueva versión del protocolo de internet.

Dirección(es) origen: varias
dirección(es) destino: varias

IGMP

Figura N° 20 Trafico IGMP (Internet Group Management Protocol)

948	328.834282	192.168.3.3	224.0.0.1	IGMP	V2 Membership Query, general
960	333.451378	192.168.20.200	239.255.255.250	IGMP	V2 Membership Report / Join gr
1289	453.809940	192.168.3.3	224.0.0.1	IGMP	V2 Membership Query, general
1291	454.447123	192.168.20.200	239.255.255.250	IGMP	V2 Membership Report / Join gr
1687	578.786242	192.168.3.3	224.0.0.1	IGMP	V2 Membership Query, general
1705	585.442596	192.168.20.200	239.255.255.250	IGMP	V2 Membership Report / Join gr
2138	703.762679	192.168.3.3	224.0.0.1	IGMP	V2 Membership Query, general
2167	712.438161	192.168.20.200	239.255.255.250	IGMP	V2 Membership Report / Join gr
2503	828.737072	192.168.3.3	224.0.0.1	IGMP	V2 Membership Query, general

Internet Group Management Protocol- Protocolo de Administración de grupos de internet: Se utiliza para intercambiar información acerca del estado de pertenencia entre routers IP que admiten el tráfico multicast y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia.

Dirección(es) origen: 00:14:d1:c2:3a:74, 00:26:22:76:d9:6c
Dirección(es) destino: 01:00:5e:7f:ff:fa(239.255.255.250),
01:00:5e:00:00:01(224.0.0.1)

IP

Figura N° 21 Trafico IP (Internet Protocol)

63446 1372.071793	10.10.0.208	255.255.255.255	IP	Fragmented IP protocol (proto=
63575 1375.061332	10.10.0.208	255.255.255.255	IP	Fragmented IP protocol (proto=
63714 1378.046411	10.10.0.208	255.255.255.255	IP	Fragmented IP protocol (proto=
63861 1381.041782	10.10.0.208	255.255.255.255	IP	Fragmented IP protocol (proto=
82404 1789.996046	10.10.0.219	255.255.255.255	IP	Fragmented IP protocol (proto=
82540 1792.972930	10.10.0.219	255.255.255.255	IP	Fragmented IP protocol (proto=
176885 3441.776334	10.10.0.208	255.255.255.255	IP	Fragmented IP protocol (proto=

Internet Protocol - Protocolo de Internet: Protocolo de capa de red encargado de transmitir información a través de una red de datos conmutados.

Dirección(es) origen: 00:0c:e7:d7:60:c0, 00:0c:e7:89:2b:d4

Dirección(es) destino: ff:ff:ff:ff:ff:ff

IPX SAP

Figura N° 22 Trafico IPX SAP (IPX Service Advertisement Protocol)

313506 7301.032172	00000000.00095b61f23b 00000000.ffffffffffff	IPX SAP	General Response
314837 7360.479524	00000000.00095b61f23b 00000000.ffffffffffff	IPX SAP	General Response
314853 7361.030771	00000000.00095b61f23b 00000000.ffffffffffff	IPX SAP	General Response
316283 7420.476357	00000000.00095b61f23b 00000000.ffffffffffff	IPX SAP	General Response
316305 7421.025868	00000000.00095b61f23b 00000000.ffffffffffff	IPX SAP	General Response
317639 7480.473261	00000000.00095b61f23b 00000000.ffffffffffff	IPX SAP	General Response
317648 7481.024080	00000000.00095b61f23b 00000000.ffffffffffff	IPX SAP	General Response
318884 7540.475475	00000000.00095b61f23b 00000000.ffffffffffff	IPX SAP	General Response
318901 7541.019592	00000000.00095b61f23b 00000000.ffffffffffff	IPX SAP	General Response

IPX Service Advertisement Protocol- Protocolo de anuncio de servicio IPX: Este protocolo sirve para anunciar, añadir y remover servicios en una red IPX.

Dirección(es) origen: 00:09:5b:61:f2:3b, 00:13:20:06:c6:b8

Dirección(es) destino: ff:ff:ff:ff:ff:ff

LLMNR:

Figura N° 23 Trafico LLMNR (Link Local Multicast Name Resolution)

790 272.163112	192.168.0.12	224.0.0.252	LLMNR	Standard query A Chicagua
791 272.263187	fe80::e9a9:e4b3:6874:ff02::1:3		LLMNR	Standard query A Chicagua
792 272.263251	192.168.0.12	224.0.0.252	LLMNR	Standard query A Chicagua
1746 600.179697	fe80::1c9b:65a2:a434:ff02::1:3		LLMNR	Standard query ANY ESSIS007
1747 600.279451	fe80::1c9b:65a2:a434:ff02::1:3		LLMNR	Standard query ANY ESSIS007
1766 604.155092	fe80::1c9b:65a2:a434:ff02::1:3		LLMNR	Standard query A Chicagua
1767 604.257104	fe80::1c9b:65a2:a434:ff02::1:3		LLMNR	Standard query A Chicagua
2061 690.151878	fe80::f493:483b:bfa0:ff02::1:3		LLMNR	Standard query A isatap
2062 690.254007	fe80::f493:483b:bfa0:ff02::1:3		LLMNR	Standard query A isatap

Link Local Multicast Name Resolution- Resolución de nombres multicast de enlace local: Protocolo de capa de aplicación que trabaja en sobre UDP y utiliza el puerto 5355 para el intercambio de mensajes. Este protocolo es equivalente al servicio NETBIOS pero para sistemas operativos vista y windows server 2008 server este soporta IPV6, el envío de resolución de nombres se hace por multicast a la dirección 224.0.0.252 o en ipv6 a la dirección multicast FF02::1:3. No es compatible con versiones anteriores de Windows.

Dirección(es) Origen: 00:23:ae:83:56:66,00:21:70:92:e1:fd,
00:13:21:1b:db:a9

Dirección(es) Destino: 33:33:00:01:00:03, 01:00:5e:00:00:fc (multicast)

LDAP

Figura N° 24 Trafico LDAP (Lightweight Directory Access Protocol)

302315	6968.855933	10.10.0.11	10.10.0.125	LDAP	bindResponse(79) success
302316	6968.856148	10.10.0.125	10.10.0.11	LDAP	SASL GSS-API Integrity: searchf
302317	6968.856444	10.10.0.11	10.10.0.125	LDAP	SASL GSS-API Integrity: searchf
302318	6968.856586	10.10.0.125	10.10.0.11	LDAP	SASL GSS-API Integrity: searchf
302319	6968.856956	10.10.0.11	10.10.0.125	LDAP	SASL GSS-API Integrity: searchf
302320	6968.857138	10.10.0.125	10.10.0.11	LDAP	SASL GSS-API Integrity: searchf
302324	6968.858683	10.10.0.11	10.10.0.125	LDAP	SASL GSS-API Integrity: searchf

Lightweight Directory Access Protocol- Protocolo de acceso a directorio ligero: Es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

Dirección(es) Origen: 00:23:ae:92:5b:dd

Dirección(es) Destino: 00:19:b9:db:da:d5

LLC

Figura N° 25 Trafico LLC (Logical Link Control)

251911	5507.995052	IntelCor_90:cb:30	Broadcast	LLC	S P, func=RNR, N(R)=64; DSAP NI
252696	5547.535631	IntelCor_90:cb:30	Broadcast	LLC	S P, func=RNR, N(R)=64; DSAP NI
252752	5550.220576	IntelCor_90:cb:30	Broadcast	LLC	S P, func=RNR, N(R)=64; DSAP NI
252753	5550.248724	IntelCor_90:cb:30	Broadcast	LLC	S P, func=RNR, N(R)=64; DSAP NI
253283	5569.446755	IntelCor_90:cb:30	Broadcast	LLC	S P, func=RNR, N(R)=64; DSAP NI
253679	5586.317593	IntelCor_90:cb:30	Broadcast	LLC	S P, func=RNR, N(R)=64; DSAP NI
253795	5592.476470	IntelCor_90:cb:30	Broadcast	LLC	S P, func=RNR, N(R)=64; DSAP NI

Logical Link Control-Control Lógico de Enlace: Protocolo de capa de enlace que define la forma en que como los datos son transferidos sobre el medio físico, proporcionando servicios a capa superiores como en este caso con Ipv6.

Dirección(es) Origen: varios

Dirección(es) Destino: broadcast ipv4, multicast ipv6

NBIPX

Figura N° 262 Trafico NBIPX (Netbios over IPX-Netbios sobre IPX)

4179	94.189124	00000000.000ffe3ace52	00000000.ffffffffffffff	NBIPX	Find name 104-08<20>
4214	95.158962	00000000.000ffe3ace52	00000000.ffffffffffffff	NBIPX	Find name 104-08<20>
4246	96.033873	00000000.000ffe3ace52	00000000.ffffffffffffff	NBIPX	Find name 104-08<20>
4280	96.907848	00000000.000ffe3ace52	00000000.ffffffffffffff	NBIPX	Find name 104-08<20>
4509	101.814085	00000000.000ffe3ace52	00000000.ffffffffffffff	NBIPX	Find name 104-08<20>
4552	102.689010	00000000.000ffe3ace52	00000000.ffffffffffffff	NBIPX	Find name 104-08<20>
4587	103.565511	00000000.000ffe3ace52	00000000.ffffffffffffff	NBIPX	Find name 104-08<20>
4747	107.518730	00000000.000ffe3ace52	00000000.ffffffffffffff	NBIPX	Find name 104-08<20>

Netbios over IPX-Netbios sobre IPX: En una red local con soporte NetBIOS, las computadoras son conocidas e identificadas con un nombre único.

Dirección(es) Origen: 00:0f:fe:3a:ce:52, 00:09:5b:61:f2:3b, 00:13:20:06:c6:b8

Dirección(es) Destino: ff:ff:ff:ff:ff:ff

NBNS

Figura N° 27 Trafico NBNS

70	19.957647	192.168.0.124	192.168.0.255	NBNS	Name query NB CHICAGUA<00>
74	20.722062	192.168.0.124	192.168.0.255	NBNS	Name query NB CHICAGUA<00>
129	43.122979	192.168.0.152	192.168.0.255	NBNS	Name query NB ZACON03<20>
131	43.873003	192.168.0.152	192.168.0.255	NBNS	Name query NB ZACON03<20>
133	44.622919	192.168.0.152	192.168.0.255	NBNS	Name query NB ZACON03<20>
182	66.613667	192.168.0.124	192.168.0.255	NBNS	Name query NB CHICAGUA<00>

Es el protocolo que define cómo se implementan los servicios de red que proporcionan aplicaciones para posterior uso de los servicios inferiores. NBT

proporciona la confianza necesaria a NetBiosAPI a través de aplicaciones para el uso del moderno protocolo TCP/IP.

NetBIOS proporciona a los programas una serie uniforme de comandos para solicitar los servicios de niveles inferiores necesarios para comunicar equipos a través de la red.

Los servicios de nombre NetBIOS (NBNS) permiten buscar la dirección IP de una máquina a partir de su nombre NetBIOS o viceversa.

Dirección(es) Origen: varios

Dirección(es) Destino: ff:ff:ff:ff:ff:ff

KRB5

Figura N° 28 Trafico KRB5 (Kerberos)

315168	7375.602755	10.10.0.125	10.10.0.11	KRB5	AS-REQ
315169	7375.614512	10.10.0.11	10.10.0.125	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH
315283	7380.050471	10.10.0.125	10.10.0.11	KRB5	AS-REQ
315284	7380.057288	10.10.0.11	10.10.0.125	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH
318043	7501.584734	10.10.0.125	10.10.0.11	KRB5	AS-REQ
318044	7501.592552	10.10.0.11	10.10.0.125	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH
318154	7507.344658	10.10.0.125	10.10.0.11	KRB5	AS-REQ
318155	7507.356125	10.10.0.11	10.10.0.125	KRB5	KRB Error: KRB5KDC_ERR_PREAUTH

Kerberos: Es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura.

Dirección(es) Origen: 00:23:ae:92:5b:dd

Dirección(es) Destino: 00:19:b9:db:da:d5

SMB

Figura N° 29 Trafico SMB (Samba)

15159	125.004552	192.168.0.13	192.168.0.90	SMB	Write Response, FID: 0x4009, 10
15158	125.004518	192.168.0.90	192.168.0.13	SMB	Write Request, FID: 0x4009, 10
15157	125.002159	192.168.0.13	192.168.0.90	SMB	Write Response, FID: 0x4009, 8
15156	125.002129	192.168.0.90	192.168.0.13	SMB	Write Request, FID: 0x4009, 8
15155	125.000493	192.168.0.13	192.168.0.90	SMB	Write Response, FID: 0x4009, 10
15154	125.000460	192.168.0.90	192.168.0.13	SMB	Write Request, FID: 0x4009, 10
15153	124.998101	192.168.0.13	192.168.0.90	SMB	Write Response, FID: 0x4009, 8
15152	124.998072	192.168.0.90	192.168.0.13	SMB	Write Request, FID: 0x4009, 8

Samba: Protocolo que configura directorios Unix y GNU/Linux (incluyendo sus subdirectorios) como recursos para compartir a través de la red.

Dirección(es) Origen: 00:26:5a:74:dc:76

Dirección(es) Destino: 00:13:d4:34:c9:48

SSDP

Figura N° 30 Trafico SSDP (Simple service discovery protocol)

103	35.248826	192.168.0.79	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
104	35.249798	192.168.0.79	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
105	35.251730	192.168.0.79	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
154	55.265251	192.168.0.79	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
155	55.266369	192.168.0.79	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
156	55.268539	192.168.0.79	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
157	55.269599	192.168.0.79	239.255.255.250	SSDP	NOTIFY * HTTP/1.1

Simple service discovery protocol- Protocolo simple de descubrimiento de servicios: Es un protocolo que sirve para la búsqueda de dispositivos UPnP en una red. Utiliza UDP en unicast o multicast en el puerto 1900 para anunciar los servicios de un dispositivo.

Dirección(es) Origen: 00:1c:f0:06:3a:fc, 00:18:39:e5:ff:f8, 00:18:39:e5:ff:f2, 00:14:d1:c2:3a:76, 00:21:70:92:e1:fd, 00:14:d1:c2:3a:74

Dirección(es) Destino: 01:00:5e:7f:ff:fa(multicast)

STP

Figura N° 31 Trafico STP (Spanning Tree Protocol)

174	62.519300	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_00	STP	MST. Root = 32768/0/00:04:0b:cf
178	64.529556	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_00	STP	MST. Root = 32768/0/00:04:0b:cf
181	66.539527	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_00	STP	MST. Root = 32768/0/00:04:0b:cf
187	68.539523	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_00	STP	MST. Root = 32768/0/00:04:0b:cf
191	70.558970	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_00	STP	MST. Root = 32768/0/00:04:0b:cf
199	72.569249	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_00	STP	MST. Root = 32768/0/00:04:0b:cf
202	74.589734	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_00	STP	MST. Root = 32768/0/00:04:0b:cf
210	76.604201	3comEuro_c9:0e:8b	Spanning-tree-(for-bridges)_00	STP	MST. Root = 32768/0/00:04:0b:cf

Spanning Tree Protocol- Protocolo de expansión de árbol: Es un protocolo de red de nivel 2, que gestiona enlaces redundantes, previniendo bucles infinitos de repetición de tramas en redes que presenten configuración redundante. STP es transparente a las estaciones de trabajo. Hay 2 versiones del STP: la original (DEC STP) y la estandarizada por el IEEE: 802.1D son incompatibles entre sí. Los bucles infinitos ocurren cuando hay rutas alternativas entre hosts. Estas rutas alternativas son necesarias debido a que, al proporcionar redundancia, dan una mayor fiabilidad ya que, al existir varios enlaces, en el caso que uno falle, otro enlace puede seguir soportando el tráfico de la red.

El problema viene dado a que al existir estos ciclos en la topología de red, las tramas broadcast y multicast pueden quedarse atrapadas en un ciclo, al no existir ningún campo TTL (Time To Leave,) en la Capa 2, tal y como ocurre en la Capa 3. Esto desperdicia capacidad de canal e inutiliza la red.

Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo del árbol que la atraviesa se reconfigura y restablece el acoplamiento activando la trayectoria de reserva. Si el protocolo falla, es posible que ambas conexiones estén activas simultáneamente, lo que podrían dar lugar a un bucle de tráfico infinito en la red corporativa.

Direccion(es) Origen: 00:1e:c1:c9:0e:8b
Direccion(es) Destino: 01:80:c2:00:00:00

TCP

Figura N° 32 Trafico TCP (Transmission Control Protocol)

540462	5484.586862	192.168.0.90	192.168.0.13	TCP	[TCP segment of a reassembled f
540463	5484.587843	192.168.0.90	192.168.0.13	TCP	[TCP segment of a reassembled f
540464	5484.587863	192.168.0.13	192.168.0.90	TCP	microsoft-ds > 1028 [ACK] Seq=
540467	5484.592999	192.168.0.90	192.168.0.13	TCP	[TCP segment of a reassembled f
540468	5484.593925	192.168.0.90	192.168.0.13	TCP	[TCP segment of a reassembled f
540469	5484.593942	192.168.0.13	192.168.0.90	TCP	microsoft-ds > 1028 [ACK] Seq=
540470	5484.593949	192.168.0.90	192.168.0.13	TCP	[TCP segment of a reassembled f

Transmission Control Protocol- Protocolo de control de transmisiones.

Protocolo que permite el transporte de tráfico orientado a conexión de manera confiable.

Direccion(es) Origen: varias
Direccion(es) Destino: varias

UDP

Figura N° 33 Trafico UDP (User Datagram Protocol)

85 25.462209	192.168.0.121	255.255.255.255	UDP	Source port: need2 Destination
93 30.462952	192.168.0.121	255.255.255.255	UDP	Source port: need2 Destination
108 35.459001	192.168.0.121	255.255.255.255	UDP	Source port: need2 Destination
123 40.459698	192.168.0.121	255.255.255.255	UDP	Source port: need2 Destination
134 45.471836	192.168.0.121	255.255.255.255	UDP	Source port: need2 Destination
146 50.461222	192.168.0.121	255.255.255.255	UDP	Source port: need2 Destination

User Datagram Protocol- Protocolo de Datagramas de usuario: Protocolo de capa de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

generado por el switch 3com con MAC 00:04:75:b5:f0:49 con destino a toda la red ff:ff:ff:ff:ff:ff.

Puerto de origen: 1048

puerto destino: 5200

Direccion(es) Origen: 00:04:75:b5:f0:49

Direccion(es) Destino: ff:ff:ff:ff:ff:ff

XID

Figura N° 34 Trafico XID (Exchange Identification)

266447 6017.796508	IntelCor_dc:fd:e8	Broadcast	XID	Basic Format; Type 1 LLC (Clas
266948 6036.356670	IntelCor_dc:fd:e8	Broadcast	XID	Basic Format; Type 1 LLC (Clas
270041 6141.523774	HonHaiPr_a0:37:90	Broadcast	XID	Basic Format; Type 1 LLC (Clas
270042 6141.526842	HonHaiPr_a0:37:90	Broadcast	XID	Basic Format; Type 1 LLC (Clas
270226 6148.733483	IntelCor_5a:cc:ed	Broadcast	XID	Basic Format; Type 1 LLC (Clas
291169 6704.427131	IntelCor_5a:cc:ed	Broadcast	XID	Basic Format; Type 1 LLC (Clas
291170 6704.428702	IntelCor_5a:cc:ed	Broadcast	XID	Basic Format; Type 1 LLC (Clas

Exchange Identification - Identificación de Intercambio: Tipo de trama LLC para tráfico no orientado a la conexión que permite informar sobre el tipo de operación y el tamaño de la ventana.

Direccion(es) Origen: 00:1e:65:72:20:d4, 00:13:ce:dc:fd:e8, 0c:ee:e6:a0:37:90, 00:1b:77:5a:cc:ed, 00:24:9f:39:96:a6, 00:1e:4c:b2:45:7b, 00:0c:e7:d7:60:c0, 00:1e:4c:86:a4:7d, 00:1a:73:4a:86:01

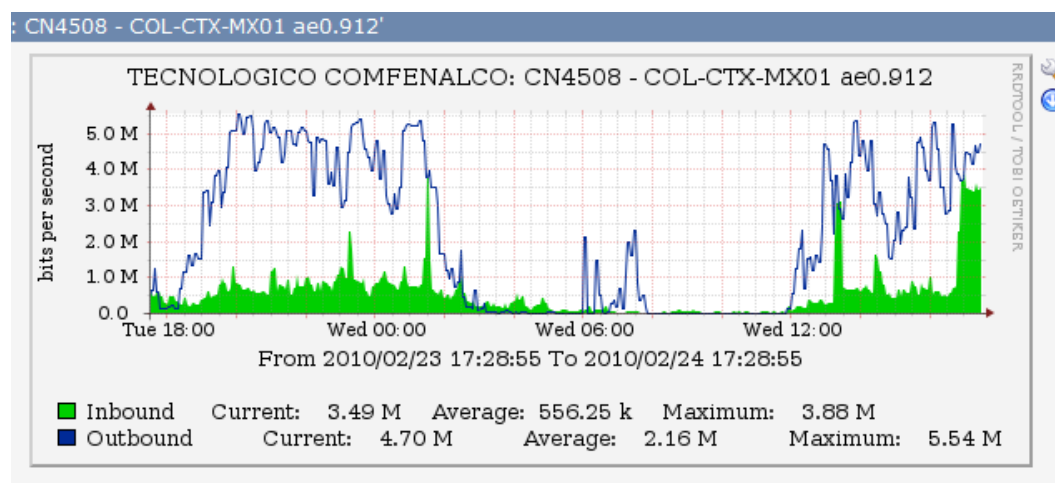
Direccion(es) Destino: ff:ff:ff:ff:ff:ff

7. DIAGRAMA DE CONSUMO DE INTERNET DE LA RED ADMINISTRATIVA Y ACADEMICA

La Fundación Universitaria Tecnológico Comfenalco cuenta con dos proveedores de Internet que son Columbus y Telefónica Telecom, con los cuales se tienen 5 MG y 4 MG respectivamente, aclaran que este último se encuentra dividido en 2 MG de datos que brindan soporte a la red académica RENATA.

A continuación se presentan una gráficas de consumo de Internet en ambas redes en horarios específicos.

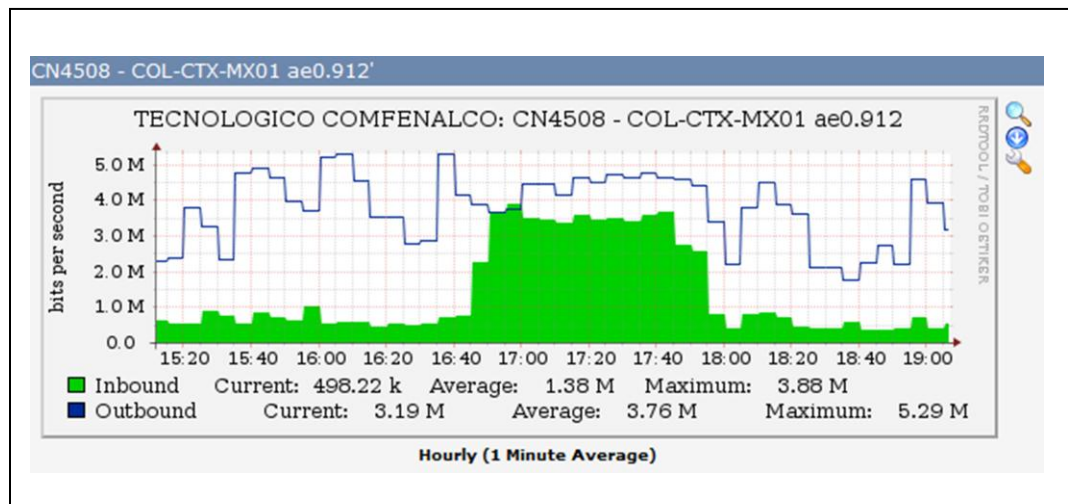
Figura N° 35 Tráfico generado por Consumo Canal de Internet



Como se poder evidenciar en la gráfica anterior se nota unos picos altos de consumos del total del ancho de banda de Columbus network, lo cual genera una disminución del rendimientos de los servicios que requieren de la Internet para su

funcionalidad, reflejándose a nivel de usuario en retrasos en las transacciones ejecutadas por los mismo.

Figura N° 36 Tráfico del Consumo Canal de Internet por hora

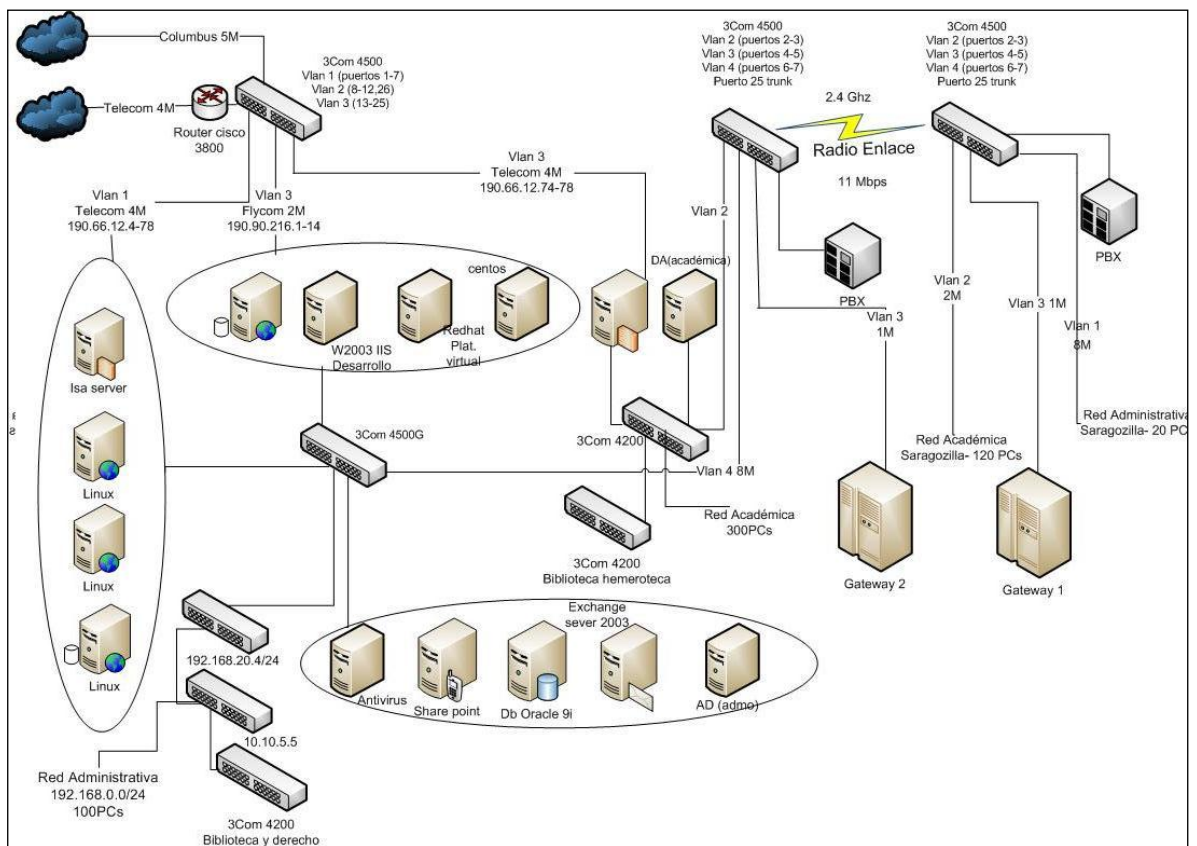


Un factor que requiere de gran atención es la realidad presentada en la gráfica anterior, dado a que la gran parte del horario nocturno presenta una constante elevada de consumo de Internet, lo que suele indicar que en estos horarios se magnifica el uso de aplicativos que requieren una alta demanda de la Internet, y que refleja una desmejora en calidad del servicio prestado.

8. ANALISIS DE TRÁFICO

A continuación se muestra en el siguiente esquema como está conformada la red de esta institución, poseen 2 canales de internet con diferentes proveedores (Columbus network 5MB y Telecom 4MB), estas conexiones llegan a un switch principal 3com 4500G configurado con 3 VLAN (aplicaciones WEB, Servidores de aplicación y Proxy), las dos sedes son comunicadas con un radio enlace que provee una velocidad de 11 Mbps por los cuales viajan las 3 VLAN configuradas como troncales (incluida aquí la voz por medio de Gateway) interconectado por unos 3com 4500G, en las dos sedes se encuentran 12 laboratorios de sistemas, cada uno con 21 equipos interconectados con un switch en cascada por sala y 200 equipos administrativos.

Figura N° 37 Diagrama Físico de Red



Microsoft Visio Software 2007

El análisis de tráfico se efectuó en la sede principal ubicada en el barrio España y en la sede de Zaragocilla, la muestra de la recolección de tráfico fue del 60% e incluyó al 90 % de los servidores ubicados en la sede principal, al 99% de los equipos activos administrables.

La recolección de los datos se realizó por medio de agentes de software del servicio SNMP habilitado en la mayoría de las maquinas muestra.

La sede principal ubicada en el barrio España cuenta con switches 4500, 4500G 3com, 4200 marca 3com, Next, Hubs 3com, planet y Encore.

Los conmutadores 4500 son de Nivel 3 y los 4200 3com, planet y Next son de nivel 2.

Los grupos administrativo y académico se encuentran asociados a una VLAN diferente cada uno (vlan 2, Vlan 4), adicionalmente existe una VLAN (vlan 3) usada para transportar tráfico de unas pasarelas voz (ATA) entre las dos sedes.

El acceso a la red pública se recibe a través de 2 operadores: TELECOM (4Mbps) vía router Cisco 3800 y COLUMBUS (5Mbps). Ambos enlaces físicos se integran a la plataforma de comunicaciones de la institución a través de 2 switches 3com 4500 que se conectan en cascada con los 4 switches principales de la capa de núcleo de la red.

La interconexión de los 4 switches de la capa de núcleo ubicados en el centro principal de cableado se hizo en cascada a través de interfaces de Gigabit.

En la misma sede se cuenta con 100 estaciones de trabajo Dell que hacen parte del grupo administrativo, 30 estaciones adicionales ubicadas en la biblioteca y en el área de derecho. También se incluyen 300 estaciones de trabajo que pertenecen al grupo académico, más 15 computadoras que soportan a los procesos servidores de:

- Bases de datos Oracle.
- Bases de datos Mysql.

- Directorio activo Administrativos/ Académicos.
- Aplicativo Sinersys.
- Servicio de consola de Antivirus.
- Servidor Web Académico
- Servicio de filtrado.
- Servidor de desarrollo.
- Plataforma Virtuales
- Servicio de Correo.
- Plataforma Antispam.
- Servidor web Corporativo.
- Servicio Proxy.

La sede principal se interconecta a la sede Zaragocilla ubicada a 870 Metros aproximadamente, a través de un enlace de radio en la banda de los 2.4Ghz implementado con equipos tipo indoor marca Linksys serie WAP54G basados en el estándar 802.11g.

En la sede Zaragocilla se cuenta con 20 estaciones de trabajo marca Dell que hacen parte del grupo administrativo y con 120 estaciones de trabajo ubicadas en las salas de informática que hacen parte del grupo académico.

Los servicios electrónicos tanto privados como públicos los reciben vía inalámbrica desde la sede principal ubicada en el barrio España.

8.1 Trafico de la red Académica

El tráfico del grupo académico tiene las siguientes características:

Tabla N° 1 Trafico de la red Académica Frame x Size

Avg Frame :	43	Frames/s	
Avg Size	122	Bytes	
Trafico WS:	5.246	Bytes/s	
#WS * SW1	24	puertos	

De manera que el trafico promedio por estación de trabajo en este grupo es de 5,246Bytes / segundo equivalente a 41,960 bits/segundo.

Siendo para la sede principal que cuenta con 300 computadoras para la red académica:

Tabla N° 2 Trafico Sede España (Frames x Sedes)

Sede Principal (España)			
# WS	300		
# Frames Sede/s	12.900	Frames/s	
#Bytes Sede/s	1.624.161.600	Bytes/s	1.6GBps
#bits Sede/s	12.993.292.800	bits/s	13Gbps

Como puede apreciarse en la tabla anterior, el trafico promedio de la sede principal es de 12,900 tramas fastEthernet/segundo lo equivalente a 12,993.292.800 bits/ segundo igual a 13 Gbps.

Considerando que los conmutadores 3com que posee la compañía tienen capacidades de conmutación de 128Gbps (4500G) y 8.8 Gbps (4500/4200) y teniendo en cuenta que los servidores se encuentran directamente conectados a un 4500G pero las estaciones que consumen sus recursos se encuentran conectadas 4500 Fast ethernet y 4200 puede afirmarse que el trafico generado excede en 4.1 Gbps la capacidad de la plataforma de conmutación de la serie 4200 y 4500 fastEthernet en situaciones en las que casi el 100% de las estaciones de trabajo requieran tener acceso a los mismos servicios (p.e Autenticación con directorio Activo).

En condiciones de distribución de tráfico normalizado, la capacidad de canal requerida se distribuye entre los switches generando necesidades de 1.039 Gbps fácilmente conmutados por los switches de la sede principal, tal como puede apreciarse en la siguiente tabla:

Ilustración 2Tabla N° 3 Trafico Sede España por SW

Sede España		
#SW	13	Unidades
Trafico X SW	1.039.463.424	1Gbps

Para la sede de Zaragoza, la situación es la siguiente:

Tabla N° 3 Trafico Sede Zaragoza (Frames x Sedes)

Sede Zaragoza			
# WS	120		
# Frames Sede/s	5.160	Frames/s	
#Bytes Sede/s	629.520	Bytes/s	
#bits Sede/s	5.036.160	bits/s	5Mbps

Según la información recolectada por los agentes referentes al tráfico de la sede Zaragocilla, las 120 estaciones asociadas a la Vlan académica generan 5.160 Tramas por segundo con un tamaño promedio de 122 Bytes para una capacidad de canal requerida de 5.036 Mbps.

Es importante tener claro que en esta sede solo se cuenta con 2 Switches. Un (1) 4500 Fast ethernet y un (1) switchs NEXT (capacidad de conmutación aproximada de 5Gbps. El resto de los equipos activos son Hubs que propagan el tráfico a sus N-1 puertos incrementado innecesariamente la capacidad de canal requerida a la vez que se expone la confidencialidad, integridad y disponibilidad de la información que transita por la plataforma de red.

Considerando esta situación podría afirmarse que la capacidad de conmutación de los switches de esta sede se encuentra casi a su limite con relación a las necesidades de trafico de las estaciones de trabajo, en situaciones en las cuales casi el 100% de los usuarios soliciten/usen recursos de forma concurrente que se encuentren en la sede principal o en la Internet.

En condiciones de tráfico distribuido, la capacidad de conmutación estaría dada por la información de la siguiente tabla:

Tabla N° 4 Trafico Sede Zaragocilla por SW /Hubs

Sede Zaragocilla		
# SW/ HUBS	5	Unidades
Trafico X SW	1.007.232	1Mbps
# Hubs	3	Unidades
# SW	2	Unidades

8.2 Clasificación del Tráfico Académico

El tráfico del segmento académico se puede clasificar de la siguiente manera:

CLASIFICACION TRAFICO

ARP/Broadcast	32,0%
IP	63,0%
UDP en IP	60,0%
NetBIOS en UDP	14,0%
Otros	5,0%
Total	100,0%

Trafico Total	12.998.328.960	13 Gbps
Broadcast Zarag.	1.611.571	1.6Mbps
Broadcast Espa.	4.157.853.696	4.1 Gbps
Broadcast Total	4.159.465.267	4.1 Gbps
Trafic No Broad Zar.	3.424.589	3.5Mbps

Puede apreciarse que el 32% del tráfico es de Broadcast, siendo 1.6Mbps generado por la sede zaragocilla y de 4.1Gbps por la sede España en condiciones de alto tráfico. Considerando esta situación puede obtenerse que los requerimientos de trafico Unicast son de 3.5Mbps + 8.8 Gbps (considerando las respuestas de los servidores a los clientes en Zaragocilla).

Es notable el efecto del broadcast como incremento notablemente en el consumo de la capacidad de canal y si a esto se le adiciona el transporte de protocolos que no prestan ningún servicio a la plataforma de red de la compañía como: IPV6, CDP, STP, que consumen capacidad de canal sin necesidad.

8.3 Trafico de la red Administrativa

El tráfico del grupo administrativo tiene las siguientes características:

Tabla N° 5 Trafico de la red Administrativo Frame x Size

Avg Frame :	64	Frames/s	SUBE A 96
Avg Size	374	Bytes	
Trafico WS:	23.936	Bytes/s	
# WS * SW1	24	puertos	

De manera que el trafico promedio por estación de trabajo en este grupo es de 23,936 Bytes / segundo equivalente a 191,488 bits/segundo.

Nótese que tanto el número de tramas promedio como el tamaño de las mismas varían con respecto al trafico académico, incluso varían entre sí para el tráfico administrativo y de los servidores. La respuesta a este comportamiento se debe a que los PAYLOAD tanto de ethernet como de muchos protocolos de capa superior sean variables, dando incluso la posibilidad a que se generen tramas conocidas como JUMBO.

Siendo que la sede principal cuenta con 100 estaciones de trabajo más 30 ubicadas en biblioteca:

Tabla N° 6 Trafico Sede España Administrativo por SW

Sede Principal (España)			
# WS	130		
# Frames Sede/s	8.320	Frames/s	
#Bytes Sede/s	4.779.540.480	Bytes/s	4.8Gbps
#bits Sede/s	38.236.323.840	bits/s	38.3 Gbps

Considerando que los conmutadores 3com que posee la compañía tienen capacidades de conmutación de 128Gbps (4500G) y 8.8 Gbps (4500/4200) y teniendo en cuenta que los servidores se encuentran directamente conectados a un 4500G pero las estaciones que consumen sus recursos se encuentran conectadas 4500 Fast ethernet y 4200 puede afirmarse que el trafico generado excede en 29,5 Gbps la capacidad de la plataforma de conmutación de la serie 4200 y 4500 fastEthernet en situaciones de alto tráfico (p.e: Descarga de Video y publicación de archivos de gran tamaño o gran cantidad de datos, trafico ARP request y reply, intercambio de mensajes DHCP concurrentes y continuos, ICMP, STP, CDP, periodo de matriculas, etc).

A pesar de que el conmutador 4500G 3com tiene capacidad de conmutar 128Gbps el resto de los switches que posee la institución, lo hace a 8.8Gbps generando la saturación de las colas (memoria), incrementando el tiempo de cpu al 95%. Situación que se ve reflejada en la pérdida de tramas y paquetes que de incluir segmentos TCP empeoran la congestión debido a la retransmisión de los mismos como parte de la implementación confiable del protocolo.

El resultado de esta situación se puede apreciar en la siguiente grafica de disponibilidad de los switches:

Figura N° 38 Disponibilidad de Switches

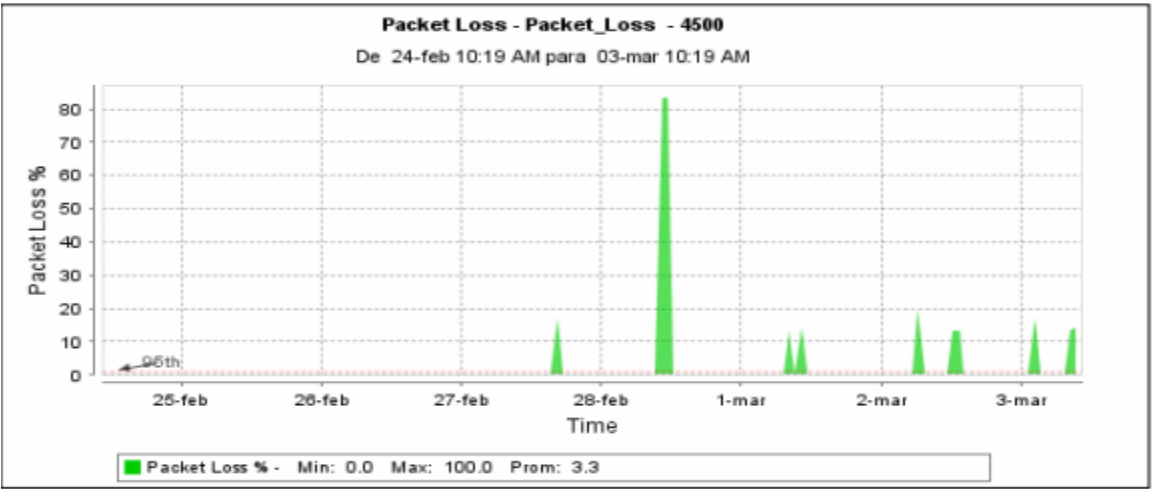


Algunos periodos de indisponibilidad detectados:

Outage History	
From	To
feb 27,2010 16:58:55	feb 27,2010 17:08:54
feb 28,2010 10:13:37	feb 28,2010 11:53:49
mar 01,2010 08:12:23	mar 01,2010 08:21:44
mar 01,2010 10:32:33	mar 01,2010 10:36:44
mar 02,2010 06:18:57	mar 02,2010 06:26:59
mar 02,2010 12:11:44	mar 02,2010 12:14:39
mar 02 2010 13:41:44	mar 02 2010 13:46:53

Igualmente puede apreciarse el porcentaje de paquetes perdidos con respecto al tiempo en algunos switches (p.e. Switch 4500 Fast Ethernet)

Figura N° 39 Trafico Switches



En condiciones de distribución de tráfico normalizado, la capacidad de canal requerida se distribuye entre los switches generando necesidades de 7.1 Gbps conmutables por los switches de la sede principal, tal como puede apreciarse en la siguiente tabla:

Tabla N° 7 Trafico Sede España Administrativo x SW

Sede España		
#SW	5	Unidades
Trafico X SW	7.059.013.632	7.1 Gbps

Para la sede de Zaragocilla, la situación es la siguiente:

Tabla N° 8 Trafico Sede Zaragocilla Administrativo Frames/Sede

Sede Zaragocilla			
# WS	20		
# Frames Sede/s	1.280	Frames/s	
#Bytes Sede/s	478.720	Bytes/s	
#bits Sede/s	3.829.760	bits/s	3.8Mbps

Según la información recolectada por los agentes referentes al trafico de la sede Zaragocilla, las 20 estaciones asociadas a la Vlan Administrativa generan 1.280 Tramas por segundo con un tamaño promedio de 374 Bytes para una capacidad de canal requerida de 3.830 Mbps.

Considerando esta situación podría afirmarse que la capacidad de conmutación de los switches de esta sede es aceptable con relación a las necesidades de trafico de las estaciones de trabajo, en situaciones en las cuales casi el 100% de los usuarios soliciten/usen recursos de forma concurrente que se encuentren en la sede principal o en la Internet. Pero la presencia de Hubs incrementa el tráfico innecesariamente y permite la aparición de colisiones en situaciones de acceso concurrente.

En condiciones de tráfico distribuido, la capacidad de conmutación estaría dada por la información de la siguiente tabla:

Tabla N° 9 Trafico Zaragocilla Administrativo SW/HUBS

Sede Zaragocilla		
# SW/ HUBS	1	Unidades
Trafico X SW	3.829.760	3.8 Mbps
# Hubs	0	Unidades
# SW	1	Unidades

El tráfico del segmento Administrativo se puede clasificar de la siguiente manera:

ARP/Broadcast	25,0%
IP	73,0%
TCP en IP	62,8%
NetBIOS en UDP	10,2%
Otros	2,0%
Total	100,0%

Trafico Total	38.240.153.600	38.3Gbps
Broadcast Zarag.	957.440	1.4 Mbps
Broadcast Espa.	9.559.080.960	9.5 Gbps
Broadcast Total	9.560.038.400	9.6 Gbps
Trafic No Broad Zar.	2.872.320	2.8Mbps

Puede apreciarse que el 25% del trafico es de Broadcast, siendo 1.4Mbps generado por la sede zaragocilla y de 9.5Gbps por la sede España en condiciones de alto trafico. Considerando esta situación puede obtenerse que los requerimientos de trafico Unicast son de 28.6 Gbps (considerando las respuestas de los servidores a los clientes en Zaragocilla e incluyendo trafico innecesario unicast como CDP,STP,IPv6, etc).

8.4 Características Equipos Activos – Conmutación

Ilustración 3Tabla N° 11 Equipos Activos y Su Capacidad

EQUIPOS ACTIVOS			
SWITCHES			
FABRICANTE	3COM	4500 G/4500/4200	
VERSION OS	v3.03.00556		
FLASH	8196	Kb	
DRAM	64	MB	
QUEUE	0-7	ROUND ROBIN	
CAPACIDAD DE SWICHING	128Gbps/8.8Gpbs		
INTERCONEXION	Cascada		
COMPORTAMIENTO CON TRAFICO			
Memoria Usada	38%	3114,48	kb
Memoria Disponible	62%	5081,52	kb
Tamaño CAM	298 DIR. MAC		
Tramas descarte prom.	37%	15,91	Tramas
Tramas Entregadas Éxito	63%	27,09	Tramas

Puede apreciarse que en condiciones de no congestión, el porcentaje de memoria principal usada es del 38% (para tareas del sistema operativo) y que el promedio de tramas descartadas es del 37% (bastante altas para condiciones normales).

Pero el porcentaje de uso de las colas está alrededor del 90% en situaciones de alto tráfico para los switches 4500 fast Ethernet, 4200 3com y superior para NEXT y Planet.

8.5 Consideraciones para el enlace inalámbrico

Tabla N° 10 equipos Enlace Inalámbrico

EQUIPOS WIRELESS			
LINKSYS WAP54G	13dbm	(-84dBm)	
ESTANDAR	802.11G	54Mbps	Indoor
ANTENAS	GRILLA	24dbi	

A pesar de que la distancia a cubrir es inferior a un (1) kilómetro, los equipos utilizados para interconectar ambas sedes son tipo INDOOR (No para soluciones inalámbricas a la intemperie) de manera que la exposición a temperaturas elevadas genera ruido térmico como efecto negativo para las comunicaciones. Incluso el hardware pobre de estos equipos genera retardo de procesamiento, que se ve reflejado en una pobre calidad de experiencia de uso del servicio por parte de los usuarios. Adicionalmente, aunque el estándar 802.11G define operación a 54Mbps como valor teórico, la capacidad de canal real es de 30Mbps promedio.

La situación se empeora debido a que los equipos están operando como bridges permitiendo que todo el tráfico de Broadcast de ambas sedes se propague por el enlace generando un incremento exponencial en los requerimientos de capacidad de canal que inducen a caídas periódicas de la solución.

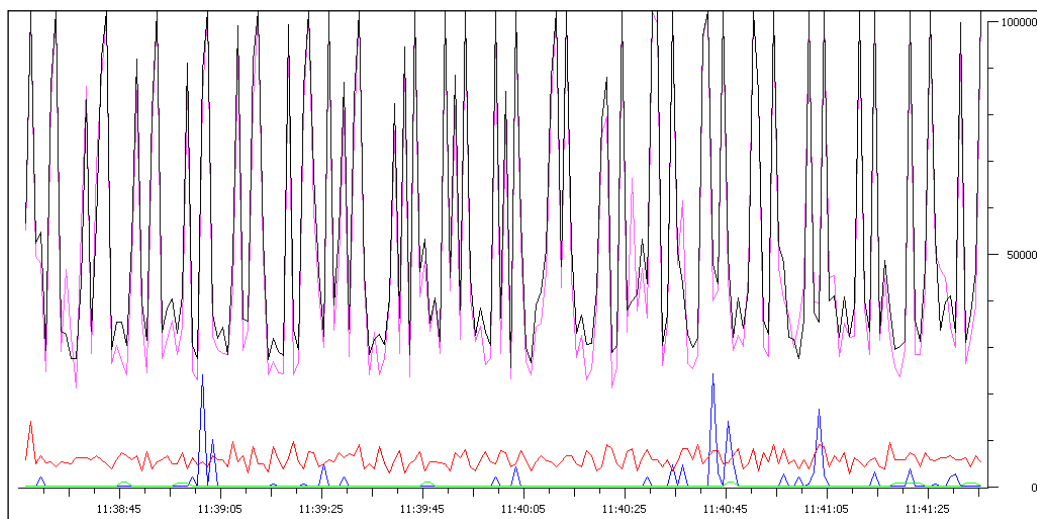
8.6 Servidores Recursos Elevados

Tabla N° 11 Servidores Críticos por Desempeño

SERVIDORES			
Servidor DB	PROBLEMA	CPU	MEM
ORACLE 9i	Desempeño	95%	94.5%
Servidor App			
SharePoint/Sinergy	Desempeño	92%	91%
PLATAFORMA VIRTUAL			
	Desempeño	90%	89%

A pesar de que el 87,5% de los servidores tienen reciben y generan tráfico, los reflejados en la tabla anterior se caracterizan por superar la media en cuanto a consumo de recursos.

Figura N° 40 Trafico Broadcast



Comportamiento normal del tráfico (número de paquetes) con relación al tiempo en periodos de alto tráfico que incluye broadcast.

Note que el tráfico de broadcast (En color Negro), supera en muchas situaciones los 10000 paquetes.

CONCLUSIONES

Después de haber realizado el análisis, con las herramientas anteriormente mencionadas, teniendo en cuenta el esquema que presenta la red y sus dispositivos, se puede sacar las siguientes conclusiones que aportaran al mejoramiento y optimización de los recursos a la empresa estudiada:

- Eliminar del tráfico de la red el protocolo STP (Spanning Tree Protocol) en la configuración de los switches.
- Eliminar el tráfico Ipv6 y el tráfico LLNMR a través de la desactivación del protocolo de Internet versión 6 en registro del sistema operativo de los clientes, ya que actualmente los clientes no están utilizando esta configuración.
- Eliminar el tráfico DHCPv6 a través de la desactivación de este protocolo en la configuración del servidor que brinda este mismo servicio para Ipv4
- Eliminar el tráfico CDP con desactivación de este servicio en el router cisco 3800.
- Cambiar el servicio DHCP para que funcione sobre un sistema operativo como Linux ya que este funciona con mensajes UNICAST y no broadcast como lo hacen todos los Windows Server.
- Revisión de la segmentación a través de Vlan ya que estas son importantes para manejar fácilmente grupos de trabajo lógicos, segmentación de los dominios de broadcast lo cual reduce el consumo de capacidad de canal, además aumenta la seguridad de las comunicaciones

definiendo cuales nodos de la red se pueden comunicar entre si a través de ACLs.

- Implementar QoS: Priorización de servicios, de flujos a través de servicios integrados o servicios diferenciados
- Evaluar el estado de red eléctrica y la puesta a tierra del centro de cableado de la sede España
- Segmentar a través de la técnica de Variable Length Subnet Mask (VLSM) toda la red para no manejar una sola IP de red y una sola IP de Broadcast por subred, segmentando así los dominios de broadcast a través del direccionamiento IP.
- Realizar enrutamiento preferiblemente estático entre la sede España y la sede de Zaragoza a través de dos routers indicados para soportar el tráfico de estas, para así evitar que el broadcast de una sede se extienda a la otra sede desperdiciando la capacidad del enlace de radio en tráfico de broadcast.
- Eliminar la conexión tipo cascada de los switches que conforman el core de la red en la actualidad y remplazarlos por un switch de core o por varios switches que permitan la realización de la conexión tipo stack para así mejorar la velocidad entre los equipos activos mencionados, y que se puedan crear ACLs y permitan manejar QOS para mejorar la calidad del servicio.
- Aumentar el ancho de banda aproximado de 5 MB, de tal manera que se aumente la probabilidad de proporcionar un mejor rendimiento de los servicios que utilizan Internet, tanto por el personal administrativo y académico de la institución.

- Implementar Firewall Perimetral y definir DMZ para los servidores Expuestos en Internet

BIBLIOGRAFÍA

- [1] Visión y Principios de la Ingeniería de Tráfico en Internet. Autores: D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, X. Xiao. Mayo 2002.
- [2] Minimum interference routing with applications to MPLS traffic engineering. Proceedings of International Workshop on QoS. Pennsylvania. Autores: M. Kodialam y T.V.Lacksham. Junio 2000
- [3] Data Networks: Routing, Security, and Performance Optimization. Capítulo 8: Quality of Service. Autor: Tony Kenyon. Año 2002.
- [4] <http://es.wikipedia.org/wiki/SMTP>
- [5] [http://es.wikipedia.org/wiki/Protocolo de Control de Transmisi%C3%B3n](http://es.wikipedia.org/wiki/Protocolo_de_Control_de_Transmisi%C3%B3n)
- [6] <http://www.rfc-es.org/rfc/rfc0793-es.txt>. Theodore John Socolofsky
Traducción al castellano: M.Angels Flores Guirola, A.J. Waisbrot (2002)
- [7] <http://telcom2006.fing.edu.uy/trabajos/mvdtelcom-002.pdf>
- [8] <http://www.wireshark.org/>
- [9] <http://timothydevans.me.uk/nbf2cifs/nbf2cifs.pdf>
- [10] http://www.cisco.com/en/US/docs/ios/12_1/configfun/configuration/guide/fcd301c.html
- [11] <http://www.javvin.com/protocolCDP.html>
- [12] <http://netcert.tripod.com/ccna/switches/cdp.html>
- [13] <http://web.mit.edu/kerberos/>
- [14] <http://www.escomposlinux.org/lfs-es/blfs-es-6.0/postlfs/mitkrb.html>
- [15] <http://personales.upv.es/rmartin/Tcplp/cap02s07.html>

LISTA DE FIGURAS

FIGURA Nº 1 MICROSOFT NETWORK MONITOR	17
FIGURA Nº 2 WIRESHARK - CAPTURA DE TRAFICO	18
FIGURA Nº 3 SNMP (MANAGER <==> AGENTE)	19
FIGURA Nº 4 DIAGRAMA DE RED (MICROSOFT VISIO SOFTWARE 2007)	21
FIGURA Nº 5 TRAFICO 0X88A7	25
FIGURA Nº 6 TRAFICO ARP	25
FIGURA Nº 7 TRAFICO BROWSER	26
FIGURA Nº 8 TRAFICO CDP - CISCO DISCOVERY PROTOCOL	28
FIGURA Nº 9 TRAFICO CLDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL)	29
FIGURA Nº 10 TRAFICO DCERPC	29
FIGURA Nº 11 TRAFICO DRSUAPI	30
FIGURA Nº 12 TRAFICO DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)	30
FIGURA Nº 13 DHCP VER 6 (DYNAMIC HOST CONFIGURATION PROTOCOL V6)	31
FIGURA Nº 14 TRAFICO DNS (DOMAIN NAME SERVICE)	31
FIGURA Nº 15 TRAFICO EPM (ENDPOINT MAPPER- MAPEADOR DE PUNTO FINAL)	32
FIGURA Nº 16 TRAFICO HTTP (HYPERTEXT TRANSFER PROTOCOL)	32
FIGURA Nº 17 TRAFICO ICAP (INTERNET CONTENT ADAPTATION PROTOCOL)	33
FIGURA Nº 18 TRAFICO (INTERNET CONTROL MESSAGE PROTOCOL)	33
FIGURA Nº 19 TRAFICO (INTERNET CONTROL MESSAGE PROTOCOL)	34
FIGURA Nº 20 TRAFICO IGMP (INTERNET GROUP MANAGEMENT PROTOCOL)	34
FIGURA Nº 21 TRAFICO IP (INTERNET PROTOCOL)	35
FIGURA Nº 22 TRAFICO IPX SAP (IPX SERVICE ADVERTISEMENT PROTOCOL)	35
FIGURA Nº 23 TRAFICO LLMNR (LINK LOCAL MULTICAST NAME RESOLUTION)	35
FIGURA Nº 24 TRAFICO LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL)	36
FIGURA Nº 25 TRAFICO LLC (LOGICAL LINK CONTROL)	36
FIGURA Nº 26 TRAFICO NBIPX (NETBIOS OVER IPX-NETBIOS SOBRE IPX)	37
FIGURA Nº 27 TRAFICO NBNS	37
FIGURA Nº 28 TRAFICO KRB5 (KERBEROS)	38
FIGURA Nº 29 TRAFICO SMB (SAMBA)	39

FIGURA Nº 30 TRAFICO SSDP (SIMPLE SERVICE DISCOVERY PROTOCOL)	39
FIGURA Nº 31 TRAFICO STP (SPANNING TREE PROTOCOL)	39
FIGURA Nº 32 TRAFICO TCP (TRANSMISSION CONTROL PROTOCOL)	40
FIGURA Nº 33 TRAFICO UDP (USER DATAGRAM PROTOCOL)	41
FIGURA Nº 34 TRAFICO XID (EXCHANGE IDENTIFICATION)	41
FIGURA Nº 35 DIAGRAMA FÍSICO DE RED (MICROSOFT VISIO SOFTWARE 2007)	45
FIGURA Nº 36 DISPONIBILIDAD DE SWITCHES	54
FIGURA Nº 37 TRAFICO SWITCHES	55
FIGURA Nº 38 TRAFICO BROADCAST	
FIGURA Nº 39 TRAFICO GENERADO POR CONSUMO CANAL DE INTERNET	43
FIGURA Nº 40 TRÁFICO DEL CONSUMO CANAL DE INTERNET POR HORA	44

LISTA DE TABLAS

TABLA Nº 1 TRAFICO DE LA RED ACADÉMICA FRAME X SIZE	48
TABLA Nº 2 TRAFICO SEDE ESPAÑA (FRAMES X SEDES)	48
TABLA Nº 3 TRAFICO SEDE ESPAÑA POR SW	49
TABLA Nº 4 TRAFICO SEDE ZARAGOCILLA (FRAMES X SEDES)	49
TABLA Nº 5 TRAFICO SEDE ZARAGOCILLA POR SW /HUBS	50
TABLA Nº 6 TRAFICO DE LA RED ADMINISTRATIVO FRAME X SIZE	52
TABLA Nº 7 TRAFICO SEDE ESPAÑA ADMINISTRATIVO POR SW	53
TABLA Nº 8 TRAFICO SEDE ESPAÑA ADMINISTRATIVO X SW	55
TABLA Nº 9 TRAFICO SEDE ZARAGOCILLA ADMINISTRATIVO FRAMES/SEDE	56
TABLA Nº 10 TRAFICO ZARAGOCILLA ADMINISTRATIVO SW/HUBS	56
TABLA Nº 11 EQUIPOS ACTIVOS Y SU CAPACIDAD	59

|